A GUIDE FOR VULNERABLE PUBLIC-FACING ORGANIZATIONS IN ADDRESSING AND MITIGATING UNWANTED ROBOCALLS

As of January 9, 2024

INTRODUCTION

This guide is based on the Hospital Robocall Protection Group's Report. The guide is intended to assist vulnerable public-facing organizations, such as hospitals and non-profit entities, in mitigating illegal calls through prevention, mitigation, and response measures. The communications industry has taken proactive steps to mitigate illegal and unwanted calls; however, vulnerable industries can also take steps in the collective effort of eliminating robocalls. The recommendations for vulnerable industries are divided by prevention as well as response and mitigation actions.

WHY ROBOCALLS ARE AN ISSUE FOR VULNERABLE PUBLIC-FACING ORGANIZATIONS?

While robocalls can be a nuisance for any individual or organization, they are particularly harmful to public-facing organizations. Public-facing organizations, such as hospitals, often exist in busy environments where staff resources are already stretched thin. As a result, these organizations are especially vulnerable to falling victim to the variety of unlawful calling schemes, ranging from phishing calls to extract sensitive information to spam calls that can overwhelm their call-processing capabilities. For a public-facing organization, like a hospital or non-profit, malicious calling activities can disrupt critical communications and render them unable to place or receive telephone calls, threaten confidential databases, facilitate unauthorized access to prescription drugs, and divert limited resources.

CURRENT INDUSTRY EFFORTS

Voice service providers are supporting the fight against robocalls with billions of unwanted calls blocked each year.[1] They have deployed:

- Call blocking and analytics tools;
- Implemented caller ID authentication technology (STIR/SHAKEN);
- And established the USTelecom-led Industry Traceback Group to support tracing, sourcing, and ultimately stopping illegal robocalls.

With the collective efforts of the government and industry, average monthly do-not-call complaints are down 35%. Also, over 90% of completed tracebacks end with the offending illegal robocaller kicked off the network or warned. The combination of industry traceback and targeted law enforcement using traceback results has proven to get illegal robocall campaigns permanently off the phone network.

- [1] E.g. AT&T - Mobile security and call protection services; Verizon - Call Filter FAQS for screening and blocking unwanted calls.

WHY ARE ROBOCALLS A PERSISTENT ISSUE?

Robocalls are pre-recorded and automated telephone calls usually delivered in mass groups. When a consumer has consented to receiving the call, these legal robocalls can help organizations provide large groups of consumers with critical and time sensitive information. In contrast, illegal robocalls indiscriminately pester consumers with a range of unlawful solicitations for products, scams, and even fraudulent and criminal activity. Despite ongoing efforts to stop robocalls for years, they remain a persistent nuisance.

Robocalls still exist because:

1. Calls can pass through multiple network providers before reaching the recipient's network, meaning the carrier can have difficulty in knowing where the call originated or if it's trustworthy.
2. The development of the internet has made it easier for people to anonymously generate millions of illegal calls.
3. The cheap costs make it easy to turn a profit.
4. The ever-evolving nature of technology available to robocall centers.

BEST PRACTICES FOR ORGANIZATIONS VULNERABLE TO ROBOCALLS INCLUDING HOSPITALS & NON-PROFIT ENTITIES

PREVENTION

Promote Education and Awareness Regarding Robocall Incidents by Training Staff to:

- Identify a robocall, recognize unlawful calls, the nature of the attack, and how to protect against scams;
- Gather key data including the date/time of the calls, number being dialed, type of calls, volume of calls, CallerID displayed, and the content of the message;
- Protect data such as personally identifiable information (PII); AND
- Be prepared to coordinate with voice service providers and law enforcement by taking the following actions:
    - Establish a governance process on how your company will work with voice service providers and law enforcement agencies.
    - Establish a plan with your voice service provider for actions to take during and after an event.
    - Determine internally through legal, compliance, and executive review the willingness of your company to report, work with and assist federal and state law enforcement agencies in the investigation and prosecution of robocall schemes.
    - 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.
    - Identify and establish relationships with designated points of contact with appropriate representatives of federal and state law enforcement and regulatory agencies.

- 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.
- Consider joining threat intelligence and information sharing organizations which offer contacts, resources, and information sharing between private industry and government.

Explore available robocall blocking capabilities to prevent fraudulent, disruptive, or nuisance robocalls, which may include:

- Reviewing with your voice service provider the current services that may be available for call labeling and blocking.
- Identifying appropriate contact information with your provider and how to respond to an unlawful robocall event, including a description of the data to collect.
- Reviewing third party offerings that may be installed in your company to assist in detecting and stopping unlawful robocall events.

Telephony management to prevent your company from being compromised

- Spoofing of number
  - Until STIR/SHAKEN is fully deployed and adopted, your company's number can be unlawfully spoofed.
  - Unlawful spoofing can be identified through random complaints reported from individuals receiving calls not originated by your company.
- 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, or no-answer rollover to other lines, etc.
  - Prevent an overload of non-critical lines from rolling-over to lines answered by key personnel.

RESPONSE AND MITIGATION

Evaluate the Event

- Determine the type of robocall event.
- Determine if the identified event is an isolated event or a part of a campaign of robocalls.
- Record 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 Where Possible

- Block spoofed numbers.
- Route to a single line extension to avoid disruption or limit the number of calls into a line extension to isolate critical phone lines.
- Separate the affected phone number from other critical trunks, which may require coordination with the PBX provider/maintainer.
- 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.

Reporting the 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 to your company and request that upstream carriers cease and desist the continued delivery of such traffic.
    - If the criteria are met, you or your provider may be able to engage the ITG to conduct a traceback to identify originating source network or end user.
- File a complaint with law enforcement
    - Complaints can be made to the FTC at the following locations:
        - DoNotCall.gov
        - ReportFraud.ftc.gov
        - IdentityTheft.gov
    - Complaints can be made to the FCC by visiting consumercomplaints.fcc.gov and clicking the link to "File an Unwanted Call Complaint."
    - 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.

- Report robocall events to your State Attorney General https://www.naag.org/naag/attorneys-general/whos-my-ag.php.

Post Filing Report

- 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.

ADDITIONAL CONSUMER RESOURCES

- FCC Consumer Guide
- USTelecom: Industry practices
- CTIA Consumer Recommendations
- FTC Consumer Recommendations