

FirstService Residential, Inc.

Robocall Mitigation Plan

For Compliance with TRACED Act

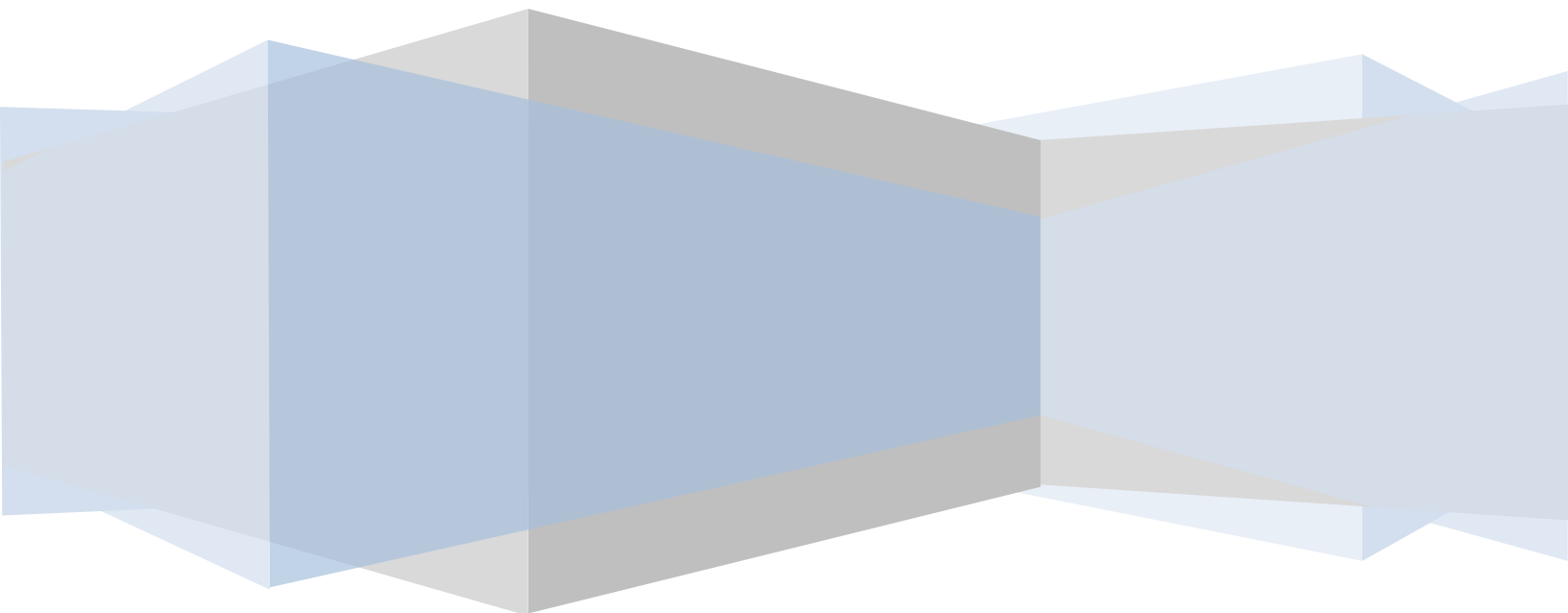


Table of Contents

DOCUMENT CONTROL HISTORY	3
1. Purpose	4
2. Scope.....	4
3. Declaration and Details.....	4
Network and Application Architecture.....	4
4. Traceback and Enforcement Cooperation	6

DOCUMENT CONTROL HISTORY

Date	Version	Description	Changed By
9/28/2021	1.0.0	Initial Document Created	Chris Cady
9/15/2022	1.2	Document reviewed	Chris Cady
9/21/2023	1.3	Document reviewed	Chris Cady
4/5/2024	1.4	Document reviewed for purposes of revised filing.	Chris Cady

1. Purpose

The purpose of this plan is to document FirstService Residential's compliance with the FCC's requirement to certify in the Robocall Mitigation Database its compliance with STIR/SHAKEN. The main goal of this effort is to ensure that illegal traffic does not originate from FirstService Residential's network.

The FCC requires voice service providers to develop a Robocall Mitigation Plan that:

- details reasonable steps to avoid originating illegal robocalls;
- shows a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls;
- and is files in the Robocall Mitigation Database.

2. Scope

FirstService Residential is a leader in property management and related services. Although it does not act as a voice service provider, it subscribes to bulk voice services from Bandwidth.com that require it to file a robocall mitigation plan.

FirstService Residential operates internally developed applications that provide calling services to its residents. These services are:

- Resident Alert – a service that allows Property Managers to (at the request of a community's board of directors) send recorded messages to residents who have subscribed to such services.
- Package Tracking Notifications – a service that calls residents to alert them to a package that has been accepted on their behalf in a central location of the property (such as the front desk of a high-rise, or the clubhouse of a gated community).

The Robocall Mitigation Plan specifically concerns the two aforementioned services.

3. Declaration and Details

Network and Application Architecture

FirstService Residential uses proprietary software to assist with managing its communities. The software (known as *Connect*) contains resident contact information such as phone numbers, email addresses and mailing addresses.

Software Access Controls

The software exposes a Resident Portal application to residents so they can see and update information pertaining to their residence. Included in this access is the ability to opt-in or opt-

out of various communications. This information is also available to authorized personnel involved in the direct management of each community.

Information is segregated on a Need-to-Know basis and access is protected with dedicated usernames and passwords.

Data/System Segregation

The services function in a protected area of FirstService Residential's data network and access databases that are housed in a non-routable vlan.

Network Security Devices

The servers that run the *Connect* application software are protected by next-gen firewalls with IDS/IPS services. All devices and network traffic are monitored for anomalies and security incidents.

Network Monitoring

All equipment is housed in a secure datacenter facility and is staffed with security services 24/7. Only specific FirstService Residential engineering associates are able to access the facility using identification badges when system maintenance is required.

Application Function/Segregation

Calls for each application (Resident Alert and Package Tracking) must be created using the application interface in the *Connect* software. This access is protected using the aforementioned controls.

Calls may only be initiated from specific whitelisted IP addresses as are declared to Bandwidth.com. Each server providing voice services for FirstService Residential is assigned a dedicated public IP address and does not share this identification with other servicers.

Server Maintenance, Security and Patching

Servers providing voice services specific to this plan may only be accessed by limited personnel and only for the purpose of supporting and maintaining their associated applications.

All services run anti-virus and anti-malware programs which are kept current with threat definitions. Servers are regularly patched to ensure they are not vulnerable to known threats. Additionally, vulnerability scanning and penetration testing are key parts of FirstService Residential's system management routine.

Service Provider Cooperation

Additionally, Bandwidth.com provides services that identify potential misuse of the network's voice services. These alerts are investigated to whether they are true or false positives. Any

malicious activity must be shut down and may result in the temporary disabling of voice services by the FirstService Residential engineering team.

4. Traceback and Enforcement Cooperation

FirstService Residential will cooperate with the traceback community, including the FCC, law enforcement, and the Industry Traceback Group to investigate and stop illegal robocalls. FirstService Residential will dedicate sufficient resources to provide prompt and reasonable responses to traceback requests.