ATIS-0300105

ATIS Standard on -

NEXT GENERATION INTERCONNECTION INTEROPERABILITY FORUM (NGIIF)

AUTO DIALERS REFERENCE DOCUMENT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0300105, *Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document*

Is an ATIS Standard developed by the **ATIS Next Generation Interconnection Interoperability Forum (NGIIF)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0300105

[Including ATIS-0300113]

ATIS Standard on

Next Generation Interconnection Interoperability Forum (NGIIF)

Auto Dialers Reference Document

Alliance for Telecommunications Industry Solutions

Approved December, 2014

Abstract

This document provides information regarding the use of auto dialers, as applicable to the ATIS Next Generation Interconnection Interoperability Forum (NGIIF).

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

The ATIS Wireless Technologies and Systems Committee (WTSC) contributed to Section 8.2, Wireless, of this document.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, Next Generation Interconnection Interoperability Forum (NGIIF) Staff, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of initiation/issuance this document, Next Generation Interconnection Interoperability Forum (NGIIF), which was responsible for its development, had the following leadership:

A. Hindman, NGIIF Co-Chair (Verizon Wireless)

M. Retka, NGIIF Co-Chair (CenturyLink)

Table of Contents

Table of Tables

ATIS Standard –

Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document

1 Scope & Purpose

1.1 Scope

This document provides information regarding the use of auto dialers, as applicable to the ATIS Next Generation Interconnection Interoperability Forum (NGIIF).

[Info from ATIS-0300113] Additionally, this document identifies best practices for Emergency Notification System (ENS) Users and ENS Vendors for time sensitive and/or emergency notifications sent through ENS systems. It addresses general basic and system information related to the use, hardware, practices, devices, and other items such as:

- ENS equipment locations, features, expansion, interoperability, configuration, and security
- Disaster recovery and business continuity procedures
- Data information, which includes data protection, integration, obtaining contact information, data collection
- Administrative and other topics from user's perspective.

1.2 Purpose

The purpose of this document is to provide a basic understanding of auto dialers such that service providers, vendors, and users of ENS equipment to understand the use of the communications network for message delivery prior to an event, so that message delivery can be optimized during times of emergency with understanding of potential impacts of network congestion.

[Info from ATIS-0300113] The guideline also provides service providers, vendors, and users of ENS equipment with best practices to optimize the delivery of time-sensitive notifications. The number of auto-dialed calls continues to rise as new technologies enable users to auto-dial thousands of phone calls every minute.

Unusual circumstances, such as an emergency event or incident, might cause a significant spike in the number of people attempting to place a phone call than is within normal bounds in addition to emergency notifications being sent via auto dialers. This document addresses educational information and best practices to consider when experiencing such an event.

Mass notification providers that lack experience working with ICT service providers to balance and throttle calls based upon what the area is likely to be able to handle may unknowingly decrease the capacity available to them and to others when they blast a large number of calls at once. This may delay recipients receiving messages and may inhibit their delivery entirely. Too few mass notification providers understand the need to proactively work with ICT service providers.

An ENS provider needs to clearly understand and have proven experience and technical expertise delivering a large number of time-sensitive calls within a concentrated area. ENS providers need to understand the importance of delivering time-sensitive notifications, routing calls and navigating network congestion, and best practices relative to usage.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-0300098, *Best Practices for Emergency Notification System (ENS) Call Volume Testing Procedure: Wireline*[1]

3 Definitions, Acronyms, & Abbreviations

For definitions of common terms used in this document, please see the ATIS Telecom Glossary, which is located at http://www.atis.org/glossary/.

3.1 Definitions

3.1.1 Access Tandem: 1. A telephone company or centralized equal access provider switching system that provides a concentration and distribution function for originating or terminating traffic between end offices and customer-designated premises. [NECA/FCC-5] 2. An exchange carrier switching system that provides a traffic concentration and distribution function for inter-LATA traffic originating/terminating within a LATA. [T1.506-1989]

3.1.2 Auto Dialer: An auto dialer is an electronic device or software that automatically dials telephone numbers either to a predetermined list or random telephone numbers.

3.1.3 Common Transport Trunk Group: A trunk group between exchange carrier switches which transports access traffic for numerous interexchange carriers concurrently and may also carry Exchange Carrier (EC) traffic. [T1.Rpt 11-1991]

3.1.4 Emergency Notification System (ENS) User/Initiator: Campus, municipality, or any other customer with ENS equipment.

3.1.5 Emergency Notification System (ENS) Provider: One who provides the ENS service.

3.1.6 Emergency Notification System (ENS) Vendor: One who provides the ENS equipment.

3.1.7 End Office: A central office at which user lines and trunks are interconnected.

3.1.8 End Office Switch: An End office Switch provides end users with telephone service, dial-tone to end users, routes calls based on the digits that the end user dials, and serves NXX codes. The network is designed so that groupings of customers share common resources (e.g., trunk groups). An End Office can serve as a host switch for one or more Remote Switching Modules (RSM). The RSM serves customers in a local community and depends on the host End Office for connection to the network.

3.1.09 Information and Communications Technology (ICT) Service Provider: Includes the interim or terminating service provider.

3.1.10 Private Branch Exchange (PBX): 1. A subscriber-owned telecommunications exchange that usually includes access to the public switched network. 2. A switch that serves a selected group of users and that is subordinate to a switch at a higher level military establishment. 3. A private telephone switchboard that provides on-premises dial service and may provide connections to local and trunked communications networks. *Note 1*: A PBX operates with only a manual switchboard; a private automatic exchange (PAX) does not have a switchboard,

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=24612 >.

a private automatic branch exchange (PABX) may or may not have a switchboard. *Note 2*: Use of the term "PBX" is far more common than "PABX," regardless of automation.

3.1.11 Public Switched Telephone Network (PSTN): A telecommunications network usually accessed by telephones, key telephone systems, private branch exchange trunks, and data arrangements. *Note*: Completion of the circuit between the call originator and call receiver in a PSTN requires network signaling in the form of dial pulses or multi-frequency tones.

The worldwide network of public switched (circuit) telephone networks is based on ITU-T Recommendation E.164 (“The international public telecommunication numbering plan”). This document is available at: http://www.itu.int/rec/T-REC-E.164/en.

As defined in ITU-T Rec. G.100, the term " (PSTN)” or, for short, "Public Network" is used for any network (without any relation to the legal status of the network operator) providing transmission and switching functions, as well as features which are available to the general public, not restricted to a specific user group. The PSTN provides access points to other networks or terminals only within a specific geographical area. From the point of view of an end-to-end connection, a public network can function either as a "Transit Network" (a link between two other networks) or as a combination of "Transit and Terminating Network" in cases where the public network provides connections to terminal equipment such as telephone sets, or PBXs.

3.1.12 Short Messaging Service (SMS): A service in mobile telephony systems that allows the user to send and receive short messages independently of voice calls; a nearly real-time service that stores messages in store-and-forward servers if the receiving mobile telephone cannot be contacted. *Note*: SMS is both the handset function and the network service. SMS is used to inform users of pending voice messages, network outages, etc., but the principal use is in user-to-user messaging. Addressing is by telephone numbers. Networks usually relay messages over network boundaries. There are gateways from e-mail and Web to SMS and from SMS to e-mail. The cost of SMS messages is usually fixed and is lower than for a short voice call.

3.1.13 Secure User Plane Location (SUPL): A set of standards defined by the Open Mobile Alliance (OMA) that provides user plane based location information for Location Based Services (LBS).

3.1.14 SaaS: Sometimes referred to as "on-demand software", is a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser.

3.1.15 Tandem Switch: A Tandem Switch serves as an aggregation point for routing traffic between End Office Switches and other Tandem Switches

3.1.16 TeleTYpe Writer (TTY): A printing telegraph instrument that has a signal-actuated mechanism for automatically printing received messages. *Note* 1: A TTY may have a keyboard similar to that of a typewriter for sending messages. *Note* 2: Radio circuits carrying TTY traffic are called "RTTY circuits" or "RATT circuits."

3.1.17 Telecommunications Device for the Deaf (TDD): A machine that uses typed input and output, usually with a visual text display, to enable individuals with hearing or speech impairments to communicate over a telecommunications network.

3.1.18 Text Messaging – A communication service that allows a user to send text messages through a telephone or via a telephone network. An example of a text messaging service might be an SMS.

3.1.19 Voice Message: The delivery of a message to the mobile device that contains a recorded audio clip which is to be subsequently played on the mobile device; either automatically upon receipt or manually via subscriber action. The key differences between text messages and voice messages are as follows:

- Different transport mechanisms on the air interface and network are used. For example, an SMS versus a MMS.
- Different media types are involved.
- Size of the message being delivered to the mobile device is much larger for voice messages than for text messages. Therefore, more network and radio resources are required to deliver voice messages than text messages.

3.2 Acronyms & Abbreviations

AT	Access Tandem
ADA	Americans With Disabilities Act (of 1990)
API	Applications Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
CERT	Community Emergency Response Teams
CMSAAC	Commercial Mobile System Alert Advisory Committee
CMAS	Commercial Mobile Alert System
COLT	Cell on Light Truck
COW	Cell on Wheels
CTI	Computer Telephone Integration
CTTG	Common Transport Trunk Group
DAS	Distributed Antenna Systems
EAS	Emergency Alert System
ENS	Emergency Notification System
EO	End Office
EOC	Embedded Operations Channel
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Administration
FTC	Federal Trade Commission
GIS	Geographic Information Systems
GSM	Global System for Mobile Communications
ISDN	Integrated Services Digital Network
IPAWS	Integrated Public Alert and Warning System
IVR	Interactive Voice Response
LATA	Local Access and Transport Area
LBS	Location Based Services
M2M	Machine-to-machine
MSC	Mobile Switching Center
MDN	Mobile Directory Number
MMS	Multimedia Messaging Service
NGIIF	Next Generation Interconnection Interoperability Forum
NOAA	National Oceanic and Atmospheric Administration
OMA	Open Mobile Access
PBX	Private Branch Exchange
PLAN	Personal Localized Alerting Network

POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RSM	Remote Switching Modules
RSS	Really Simple Syndication
SaaS	Software as a Service
SLA	Service Level Agreement
RATT	Radio Automatic Teletype
RTTY	RadioTeletype
SMS	Short Messaging Service
SS7	Signaling System 7
SUPL	Secure User Plane Location
TDD	Telecommunications Device for the Deaf
TTY	TeleTYpe Writer
VPAT	Voluntary Product Accessibility Template
VoIP	Voice over Internet Protocol
WARN	Warning, Alert and Response Network
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Service
WTSC	ATIS Wireless Technologies and Systems Committee

4 What Are Auto Dialers?

An auto dialer is an electronic device or software that automatically dials telephone numbers either to a predetermined list or random telephone numbers. When the call is answered, then the auto dialer plays either a recorded message, connects to a live person, may play a recording then connect to a live person, or provide a menu of options. An auto dialer may also be programmed to send short text messages to the target telephones or to leave a message on voicemail or telephone answering systems when those devices are activated. Auto dialers are an example of Computer Telephone Integration (CTI). Auto dialers can be used both over PSTN or Voice over IP (VoIP).

4.1 Names/Aliases of Auto Dialers

Auto dialers can be referred to by many different names. Some examples are auto dialers, predictive dialers, power dialers, robocalls, voice broadcasting, telemarketing dialers, Tele-Town Halls™, war dialing, VoIP dialers, and Emergency Notification Systems (ENS). A more complete list can be found in Annex A, Types of Auto Dialers & Definitions.

5 How Do Auto Dialers Work?

Auto dialers can vary greatly. They can be simple or very complex systems with many features. A basic system consists of four components: A computer, usually and preferably a desktop, a voice modem, auto dialer software, and an active telephone line. A typical desktop computer may have multiple modem cards with each one connected to a single phone line, or may use an internet connection. More modems mean more calls can be placed simultaneously. The most important part of the auto dialer system is the software. The software determines the numbers to call and how to react to the various call terminations (e.g., answering machines, live person, busy signal, voicemail, etc.)

There are three basic variations of auto dialers: one that leaves a pre-recorded message, one that connects end users to a live operator, and one that sends out short text messages. An auto dialer that plays a pre-recorded message may be called a "robocalling" or "voice broadcasting" auto dialer, or be referred to as "robotexting". An auto dialer that connects the answered call to a live agent may be called a "predictive" auto dialer or "power dialer". Mass sending of short text messages is one of the normal (but not exclusive) operating modes of notification systems.[2]

Instead of purchasing or assembling an auto dialer system, there are auto dialer services that can be used to generate voice notifications. Campaigns can be initiated by providing announcements, interactions, phone numbers or calling pattern, and payment arrangements to the auto dialer servicer provider, often using a web site.

5.1 Robocalling/Voice Broadcasting

Robocalling/voice broadcasting is the most common form of an auto dialer service. It is typically used for calls related to sales, marketing, or polls. When an opinion or some other type of poll is being conducted the pre-recorded message may ask the answering person to press a digit on their phone pad, or respond with a specified text, if the recipient supports a particular side of an issue, or another phone digit or text if the recipient supports an alternative side.

Robocalling may also be used to scam consumers or for illegal purposes. Consumers may receive phishing calls, focused nuisance attacks, call flooding, or Denial of Service (DoS). Service providers, industry standards bodies, the FCC, and the FTC work cooperatively and independently to mitigate these types of illegal calls.

Services providers and private entities are developing or have current services and features available to consumers to address illegal robocalls.

Another common use is for notifications, announcements, or reminders. This is frequently used by Public Safety officials via a system called an Emergency Notification System (ENS). ENS is addressed in Section 9, Best Practices for Emergency Notifications.

5.2 Predictive / Power Dialer

Depending on the software, the computer can detect whether a live person answers, and then transfer the interaction off to a live agent at that time. This would typically be called voice detection. A predictive dialer uses real-time analysis to determine the best time to dial more numbers. A power dialer dials a pre-set number of phone lines to provide a live agent with a new call once the agent finishes the previous call.

6 Who Uses Auto Dialers & How Are They Being Used?

Auto dialers are used by many different groups for a variety of reasons. Examples of these groups are: community or private organizations, politicians, businesses, schools and agents of states, and counties and cities.

Advanced notifications are desirable prior to placing a mass calling notification event. In many cases, it is not practical due to the nature of some types of events, such as emergencies. However, it would be helpful if agreements and arrangements could be made between the local service provider and the mass calling operator to have the first call in the notification queue go to a number designated by the service provider. This alert to the

[2] See 4GAmerica, "Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services" September 2008, < http://www.4gamericas.org/index.cfm?fuseaction=page&sectionid=428>.

local service provider at the initiation of the event may assist in giving the service provider advanced awareness of a mass calling event.

6.1 Community or Private Organizations or Businesses

Community or private organizations or businesses use of auto dialers have commonly been referred to as telemarketing. Telemarketing applications may include charities to raise money or businesses generating calls to solicit business, etc. Frequently, this type of auto dialer use is an automated call which when answered is transferred to a live operator who will make the ‘sales, charity, or business’ pitch.

6.2 Schools

Schools, at all levels, have found the use of auto dialers to be an efficient means to provide information to students and parents. Some examples are: delayed openings and early closings, weather delays, traffic information, report card notices, sports events, fundraisers, and extracurricular activities.

ENS is one type of a notification system that colleges and universities may be adopting. Colleges or universities use notification systems for emergencies, non-urgent or real-time events such as school closings, weather and traffic.

6.3 States, Counties, Cities, Towns, Villages, Public Utility

Government entities, such as states, counties, cities, towns and villages are adopting the use of auto dialers for many applications. Some of those uses include public service messages, parade notification, road closures, construction notices, fundraisers, local events, public utility messages, boil order notices, water contamination, or water shut off notices. ENS is also being used by government entities to notify residents of localized events such as burglaries in a specific neighborhood, notification of scam artists operating in an area or municipality, weather emergencies, activation of Community Emergency Response Teams (CERT), large area fires, etc. Government entities may also use ENS for situations that could be classified as non-emergency.

6.4 Politicians

Politicians are increasingly turning to auto dialer type systems as a means to get their information to a large population of voters in an inexpensive and timely manner.

A politician may use several different kinds of auto dialer types; one example is a “Town Hall” application. A politician will utilize an auto dialer to gather a large group of their constituents by the system calling them individually, inviting them to attend a town hall conference currently in progress. Constituents who wish to attend indicate so by pressing a specified digit on the telephone number pad and then are placed into the on-going discussion led by the politician. Many of these systems have options where the constituent can ask questions. Questions can also be asked privately where the politician can respond at a later time.

Another type of auto dialer use is where a politician records a brief message which is sent to a list of constituents. This is typically a one-way communication.

6.5 Scammers & Phishers

Scammers and phishers may use auto dialer robocalling to expand the number of targets they reach in their efforts to illegally obtain consumers’ personal or financial information with the intent of perpetuating fraud on the consumer. They may also use robocalling to flood bank or other anti-fraud services, rendering them temporarily unavailable to victims.

7 How Auto Dialers Impact Telecommunications Networks

High volumes of calls generated by mass call systems have significant impact on service provider telephone networks. Those impacts can range from mild to catastrophic, depending on scope and circumstances of the event. Those impacts can affect network integrity, customer service, revenues of both customers and service providers, and in certain circumstances, present a threat to life sustaining services. For these reasons, the telephone industry works to maintain the integrity of and minimize impacts to the nation's network.

7.1 Telecommunications Network Overview

The PSTN is a compilation of networks operated by different providers that work together to complete a call. A network is comprised of many different elements such as:

- End Office (EO) Switch – An end office switch provides end users with telephone service, dial-tone to end users, routes calls based on the digits that the end user dials, and serves NXX codes. The network is designed so that groupings of customers share common resources (e.g., trunk groups). An End Office can serve as a host switch for one or more Remote Switching Modules (RSM). The RSM serves customers in a local community and depends on the host End Office for connection to the network.
- Tandem Switch – A Tandem Switch serves as an aggregation point for routing traffic between End Office Switches and other Tandem Switches.

When the use of an auto dialer targets a particular EO, the common resources are overloaded. The overloads can occur:

- On the Common Transport Trunk Group (CTTG) between the Access Tandem (AT) and the local EO
  - The Common Transport Trunk Group is a two-way group that connects an EO to the Access Tandem (AT). A blockage on this group affects all traffic which includes the auto dialer generated calls. Blockages on these trunk groups are routed to an "All Trunks Busy" announcement.
- On the channels between incoming trunks and line equipment
  - Channels are part of the switch mechanism. There are limited amounts of channels between incoming trunk equipment and line equipment. Calls blocked at this stage of the call are routed to an announcement that advises the caller that the call failed.
- On intercept trunk groups because of numerous calls to vacant numbers
  - Intercept trunk groups connect the call to an announcement circuit to inform the caller that the line number they dialed is not in service. When intercept trunk groups are overloaded, this service is not available to customers dialing the changed or disconnected number.
- When the specific announcement trunks are all busy the calls are routed to T120, more commonly referred to as "fast busy" or Reorder.

If the terminating tandem or EO has exhausted its announcement trunks, it will begin to advise interconnected switches to temporarily curtail traffic destined for its serving area. This will affect all traffic between the terminating switch and all switches interconnected with that switch.

If the terminating numbers are served by an RSM, it is possible that the blockage at the terminating tandem or EO will isolate the remote office. An isolated RSM without local emergency services would result in customers served from that RSM being unable to contact emergency services that are located outside of the RSM coverage area.

All of the scenarios referenced here could result in the blockage of originating or terminating emergency calls.

Both SS7 and IP-based networks support system control and network congestion protocols; however, the control levels for IP-based networks are continuing to be developed. Also, many of the network congestion protocols are designed toward blocking calls to a single number, such as radio station contests. The major problems created with the use of auto dialer systems is the inverse, where a single number is calling many numbers.

7.2 Wireless

This section discusses the technical and subscriber aspects, which may have significant differences, related to a voice-based notification service based upon wireless telephony. This voice-based notification service is initiated by a third party server with the intent to send voice notifications to individuals within a specific notification area. These voice notifications could either be for emergency situations (e.g., spreading wildfires) or a community notification (e.g., community carnival). The principles addressed in this section should apply for any type of auto dialer type system based upon wireless telephony services.

7.2.1 Technical Differences between Wireline & Wireless Networks

Table 7. 1 - Technical Differences Between Wireline and Wireless Networks

Network Attribute	Wireline Networks	Wireless Networks
Number of telephone devices within the notification area.	Could be determined from any database with addresses and telephone directory numbers.[3]	Cannot be determined. Any domestic or international mobile devices could be within the notification area. Mobile devices may include more than cell phones, including but not limited to tablets, wireless modems, machine-to-machine (M2M) connections. Alternative services such as VoIP may be used on devices other than cell phones, and therefore could be affected by auto dialers. There can be major fluctuations on the number of devices within the notification area based upon emergency/ disaster conditions or based upon preplanned events such as football games, street fairs, or other large gatherings.
Directory numbers of the telephone devices within the notification area.	Can be roughly estimated from any database with addresses and telephone directory numbers.[4] Some devices may be remotely located VoIP devices, or virtual numbers that forward calls to other locations.	Cannot be determined. No national or international directory exists with mobile numbers. Any domestic or international mobile numbers could be within the notification area at a given time period. The communications are shifting from wired to wireless and the notification systems have to be modified to adapt to this shifting communications model. There is a large and growing number of households that are wireless only.

[3] Address and telephone directory number databases could be populated from a variety of sources including self-registration. During self-registration, the telephone directory numbers added to a database could either be wireline or wireless numbers.

[4] Address and telephone directory number databases could be populated from a variety of sources including self-registration. During self-registration, the telephone directory numbers added to a database could either be wireline or wireless numbers.

Network Attribute	Wireline Networks	Wireless Networks
Volatility of network configuration.	Network changes occur based upon the provisioning of additional, changed, or deleted wireline telephone services.	Network changes could occur frequently and dynamically to adjust to shifting traffic conditions. The wireless network continues to grow in terms of deployment of a vast number of cell sites in the US.[5] Temporary cell sites such as Cell on Wheels (COW) or Cell on Light Truck (COLT) could be established for anticipated network congestion conditions such as football games, street fairs, or other large gatherings. Additional types of cell sites may include Distributed Antenna Systems (DAS) and small cells (e.g., femtocells) the number of cell sites continue to grow.
Current location of telephone device	Can be determined from any database with addresses and telephone directory numbers.	A signal is sent to the mobile device via the network to determine if it is still within the last known location. The results of this request will indicate the cell site currently serving the mobile device. For higher accuracy location information, either SUPL (Secure User Plane Location) protocols or emergency 9-1-1 location determination protocols could be used on a per mobile device basis. The determination of mobile device location to FCC regulations for emergency 9-1-1 calls can take up to 30 seconds per mobile device using very sophisticated techniques such as radio signal triangulation methods. More information is available on the OMA web site at http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases.
Traffic load prediction	Based upon telephony traffic engineering techniques based upon known number of telephones and desired blocking factors.	Based upon historical busy hour traffic volume statistics which vary by hour, by day, by cell site, and by location. Additionally, the increased use of data among mobile subscribers can greatly affect traffic volumes, and may significantly differ from historical traffic patterns. The wireless network continues to grow in terms of deployment of a vast number of cell sites in the US.[5]

[5] http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts

Network Attribute	Wireline Networks	Wireless Networks
Association of billing address to telephone location	Telephone device may not be at same location as the billing address.	Billing address has no relationship to location of mobile device. Mobile devices with a pre-paid wireless service have no associated billing address.

7.2.2 Impacts of Wireless Services to Voice-Based Notification Services

Incoming telephone calls are routed based on the wireless subscriber's Mobile Directory Number (MDN) and then terminated on the subscriber's wireless device, regardless of the subscriber's current location. This characteristic of wireless services has the following impacts on voice-based notification services:

- It is virtually impossible for the voice-based notification service to determine the location of the wireless subscribers on their notification list.
- It is virtually impossible for the voice-based notification service to determine which subscribers who live, work, or attend school in the desired notification area are within the notification area when the voice-based notification is to be sent.
- It is virtually impossible for the voice-based notification service to determine what other wireless subscribers from other communities, other service providers, or other countries may be roaming within the desired notification area.
- Incoming voice notification telephone calls are delivered to the wireless subscriber at any location within the city, state, country or even internationally (if the subscriber has an international calling service). The wireless subscriber may have to pay charges for these incoming voice-based notification calls depending on the subscriber's current location and on the subscriber's service plan.

NOTE: If the wireless subscriber(s) is on a service list, location of the subscriber when the notification goes out would be irrelevant, as the notification would be sent to everyone on the list. However, if there is no list involved with a given notification, most likely everyone in that area (however the area is defined for notification purposes) would receive the notification, i.e., all those homed off the cell sites within the "area." The notifier could not determine who does and does not receive the message. These situations could have implications associated with roaming.

7.2.3 Network Engineering for Wireless Networks

Wireless networks are engineered to minimize network congestion conditions which could impact the ability of the subscriber to make and receive telephone calls. The wireless networks are engineered based upon historical busy hour traffic volume statistics which vary by hour, by day, and by location. The engineering of wireless networks is based on the theory that the future behavior of the network will be similar to past behavior and include a small margin for network growth. Wireless network congestion will occur whenever actual conditions exceed these assumptions and an alternate route is not available. The magnitude and scope of the network congestion depends on the magnitude and scope of the associated event.

NOTE: Any broadcast event sent to the public could result in an exponential increase of traffic over the wireless and/or landline network to notify others or a request to public service for clarification. In other words, even if the broadcast itself does not cause network congestion, it is possible that the public's reaction to the notification could cause network congestion.

7.2.4 Network Congestion Conditions Well Known to Wireless Operators

The network behavior and impact to subscribers under conditions of network congestion are well known to the wireless operators based upon actual events. The following are examples of network congestion conditions from actual events:

- Cell sites covering the area of the Minneapolis I-35W bridge collapse.
- New Year's Eve at Times Square.
- New Orleans after Hurricane Katrina.
- Emergency calls to 9-1-1 in eastern states during Hurricane Irene.
- Large festivals or sporting events.

Due to the mobile nature of wireless subscribers, an action or event in one place could cause a network condition in a different part of the network which is not related to the location of the action or event. An example of this type of condition is described in Section 7.2.7, *University Notification System Example*.

7.2.5 Potential Subscriber Impacts from Network Congestion Conditions

Network congestion conditions including those caused by a voice-based notification system will have impacts to other subscribers and other services as follows:

- Other wireless subscribers not associated with the voice-based notification system but whose calls originate on the same cell sites may not be able to make or receive calls
- Wireless 9-1-1 emergency calls could be blocked. There is no priority allocation of resources for 9-1-1 emergency calls.
- Wireless services for first responders via the Wireless Priority Service (WPS) could be blocked or delayed. Since FCC regulations do not allow for preemption of voice calls, any first responder's calls via WPS would have to be queued for next available resource.
- In addition to congestion of the wireless access resources, wireless networks are subject to the same type of congestion of common resources (interconnecting trunk groups, announcement systems, etc.) due to the action of voice-based notification systems that can affect the PSTN. For example, a campaign that includes a significant number of wireless customers can overload the trunks between the PSTN and the wireless network, which can impair the ability of wireless customers to make or receive calls to users served by other networks.
- Voicemail systems could become overloaded to the increased number of telephone calls including voice-based notification calls that are being diverted to voicemail. Consequently, during overload conditions of the voicemail systems, any subscriber may not be able to retrieve stored voicemail messages and incoming calls for any subscriber may not be able to store in the subscriber's voicemail box.

7.2.6 Wireless Subscriber Expectations

The expectations and demands of wireless subscribers can be different than those of wireline subscribers. These types of differences need to be considered for any services which might involve wireless subscribers.

7.2.6.1 Tolerance to Unwanted Calls

Wireless subscribers may be less tolerant to receiving calls which in the view of the subscriber are considered to be annoyance calls, telemarketing calls, or unsolicited calls, due to the way in which wireless subscribers are charged for incoming and outgoing calls. Wireless subscribers could consider voice-based notification calls to be in this category especially for non-emergency notifications and their reactions could be any or all of the following:

- Ignore or block all calls from the originating entity (*e.g.*, city, university, and voice-based notification service). However, the subscriber will not receive the emergency voice-based notifications because they have been overloaded with too many other notifications which were deemed to be worthless by the subscriber.
- Unsubscribe from the sign-up list of the originating entity.

- Complain to the originating entity (*e.g.*, city, university).
- Complain to the wireless operator about these annoying calls and request methods to block these calls.
- Complain to the state Public Utilities Commissions or to the FCC.

7.2.6.2 Potential Associated Subscriber Cost Impacts

The potential associated subscriber cost is one reason why wireless subscriber expectations are different from the wireline subscriber expectations. Depending upon the subscriber's wireless service plan, the wireless subscriber could incur the following types of charges when they receive voice-based notification calls:

- National and/or international roaming charges when the subscriber is outside the intended notification area.
- Depletion of available minutes on postpaid wireless accounts which could cause additional expense to the subscriber if available monthly minutes are depleted before the end of the monthly cycle.
- Depletion of account balance on prepaid wireless phone accounts.

Calls should be coded to avoid these costs.

7.2.6.3 Potential False Expectations by Wireless Subscribers

The wireless subscriber could also have a false set of expectations for a wireless voice-based notification system. The following are some examples of these false expectations:

- A subscriber lives in a community which has implemented a voice-based notification service to wireless devices. This service works for the subscriber when at home and has received several notifications. If the notification wireless directory number list is created by some method that did not require a sign-up process, the subscriber might have the expectation that this notification service would also automatically work for any out of town visitors. This expectation might be incorrect if the community or the voice-based notification service does not know which wireless subscribers are in the desired notification area, unless the voice-based notification service receives a real-time feed from the cell site(s) within the community. It is more likely that the notification would be based on the Mobile Switching Center (MSC) the cell site is homed to, because the cell site holds limited information. The scenario is more likely to be based on a notification to a specific area or areas through the MSC, in turn, the MSC would broadcast to the cell sites identified in those areas, and then a broadcast would be sent to all mobile devices connected to those cell sites.
- A subscriber is visiting another community which has implemented a voice-based notification system to wireless devices. The subscriber would assume that voice-based notifications would be automatically received. This expectation might be incorrect if the community or the voice-based notification service does not know that the subscriber is now located within the notification area, unless the voice-based notification service receives a real-time feed from the cell site(s) within the community. It is more likely that the notification would be based on the MSC the cell site is homed to, because the cell site holds limited information. The scenario is more likely to be based on a notification to a specific area or areas through the MSC, in turn the MSC would broadcast to the cell sites identified in those areas, and then a broadcast would be sent to all mobile devices connected to those cell sites.

7.2.6.4 Support for Individuals with Disabilities

Emergency notification services included as part of voice-based notifications need to address the needs of individuals with disabilities (e.g., visually impaired, hearing impaired). For example, the Commercial Mobile Alert System (CMAS) incorporates dedicated audio alert tones and vibration cadences which provides benefit to all subscribers as well as supporting the needs for individuals with disabilities. However, emergency voice-based notification calls cannot be distinguished from ordinary calls. Consequently, subscribers, especially the individuals with disabilities, cannot distinguish emergency calls from other calls. TTY/TDD can be set up to broadcast emergency notifications. Some TTY users use specific vibration “codes” to identify callers as others might use distinct ring tones.

NOTE: The support of TTY/TDD in 3GPP is defined in Global Text Telephony (GTT). GTT covers both emergency and non-emergency calls for TTY/TTD devices. The Stage 1 specification for GTT is 3GPP TS 22.226 and the Stage 2 specification is 3GPP TS 23.226.

7.2.6.5 Subscriber Behavior in Emergency Situation Considerations

The behavior of subscribers in an emergency situation must also be considered. For example, when subscribers receive a life threatening emergency event notification via a voice-based notification service, the subscribers have their mobile device in their hand and the first action that could happen is to immediately attempt to contact others *via* their mobile device to make sure they are aware of the emergency situation. If the subscribers are unable to reach their friends or loved ones, they may continue to retry calling them for at least as long as the life threatening emergency event continues. Voice-based notification to other subscribers may still be in progress when the first subscribers who have already been notified are attempting to contact their friends and loved ones. The combination of the voice-based notification service in conjunction with the subscribers’ expected behavior will accelerate the network utilization to the conditions of network congestion and will extend the amount of time required before the network utilization decreases below network congestion levels.

NOTE: Any broadcast event sent to the public might and could result in an exponential increase of traffic over the wireless and/or landline network to notify others or a request to public service for clarification. In other words, even if the broadcast itself does not cause network congestion, it is possible that the public’s reaction to the notification might cause network congestion.

7.2.7 University Notification System Examples

Below are examples of voice-based and text-based notification systems.

7.2.7.1 University Notification System Example – Voice-Based Notification System

To illustrate the principles and issues that have been presented above, this section discusses an example of a voice-based notification system for a university. For this example, the following items are assumed:

- The university has a large number of students and staff members.
- The majority of university students and staff members have wireless phones.
- The university is located within an urban area.
- The university campus is surrounded by other businesses and residences.
- Major highways and thoroughfares are adjacent to campus.
- The university has built a list of the wireless directory numbers using university databases of faculty and student information.

The university has initiated a voice-based notification and as a result any or all of the following could occur:

- Network congestion could occur on the limited number of cell sites covering the university campus.
    - University students and faculty could be unable to make or receive other calls including 911 calls.
    - Neighboring businesses and residences could be unable to make or receive wireless calls including 911 calls.
    - Subscribers traveling on the adjacent highways and thoroughfares could be unable to make or receive wireless calls including 911 calls.

  - Existing calls of subscribers traveling into the cell site coverage area of the university could be disconnected. This would include any subscribers on the adjacent highways and thoroughfares.

- Any university students or faculty members outside of the university campus area would also receive the voice-based notification. These subscribers could incur additional charges. These subscribers could also be annoyed because the voice-based notification calls occurred in the middle of the night at their current location.
- Visitors to the desired notification area of the university would not receive the voice-based notification calls.
- If a large number of the university students and faculty members are concentrated in another location other than the university campus (e.g., the football stadium of another university) when the voice-based notification is being sent, the initiating university could be causing network congestion conditions at a location away from their own campus. This network congestion could affect the other university as well as its surrounding businesses, residences, highways, and major thoroughfares.

7.2.7.2 University Notification System Example – Text-Based Notification System

To illustrate the principles and issues that have been presented above, this section discusses an example of a text-based notification system for a university. For this example, the following items are assumed:

- The university has a large number of students and staff members.
- The majority of university students and staff members have wireless phones.
- The university is located within an urban area.
- The university campus is surrounded by other businesses and residences.
- Major highways and thoroughfares are adjacent to campus.
- The university has built a list of the wireless directory numbers using university databases of faculty and student information.

The university has initiated a text-based notification and as a result any or all of the following could occur:

- Network congestion could occur on the limited number of cell sites covering the university campus.
  - University students and faculty could be unable to send or receive other text messages and/or make or receive voice calls, including 911 calls.
  - Neighboring businesses and residences could be unable to send or receive other text messages and/or make or receive voice calls, including 911 calls.
  - Subscribers traveling on the adjacent highways and thoroughfares could be unable to send or receive other text messages and/or make or receive voice calls, including 911 calls.
  - Existing calls of subscribers traveling into the cell site coverage area of the university could be disconnected and/or wireless subscribers may not be able to send or receive text messages. This would include any subscribers on the adjacent highways and thoroughfares.
- Any university students or faculty members outside of the university campus area would also receive the text-based notification. These subscribers could incur additional charges. These subscribers could also be annoyed because the text-based notifications occurred in the middle of the night at their current location.
- Visitors to the desired notification area of the university would not receive the text-based notifications.
- If a large number of the university students and faculty members are concentrated in another location other than the university campus (e.g., the football stadium of another university) when the text-based notification is being sent, the initiating university could be causing network congestion conditions at a

location away from their own campus. This network congestion could affect the other university as well as its surrounding businesses, residences, highways, and major thoroughfares.

7.2.8 Mass Notification Methodology Studies

Mass notification methodologies have been studied by various groups including ATIS WTSC, GSM Association, ETSI, 4G Americas, and the FCC Commercial Mobile System Alert Advisory Committee (CMSAAC). All of these groups have reached the same general conclusion that point-to-point communications methods such as separate voice messages and/or voice calls to each individual are not feasible or practical.

CMAS will support delivery of a short text message (up to 90 characters) to all compatible mobile devices within a targeted geographic area. CMAS will use a “broadcast channel” within the mobile command/control spectrum to distribute the same alert to all handsets using common frequency resources. This design minimizes the impact that would occur if the regular text messaging resources of mobile networks were used to deliver the alert. Devices must be designed to receive CMAS messages.[6]

7.3 VoIP Networks

Networks that use VoIP can also be affected by auto dialers. VoIP networks include IP routers, call control servers, application servers, media servers and gateways. When the use of an Auto Dialer targets a particular VoIP network, the resources can be overloaded. The overloads that can occur include:

Network elements such as media servers and call control server:

- The number of active sessions the server can support can be exceeded, or the volume of call requests may exceed the processing capacity of the server. These limits may be real or virtual (the provider may only have licensed a certain call volume from the vendor). When the call server’s capacity is reached, no further calls can be made to or from users served by that call server, even if there is sufficient bandwidth for additional call paths.

Network elements such as routers and gateways:

- There is a limited amount of bandwidth between the edge of the network and the user equipment. When overloaded, there may be no available bandwidth to support an audio stream even if the call control server can process the call request. When bandwidth is exceeded users may not be able to hear the other party (or announcement) even though there may be signaling to set up the call.

Unlike the PSTN, in some VoIP networks users may share a common access medium (as in a cable network). This may also present another bandwidth resource which may be subject to overload.

VoIP networks can experience overload behaviors that do not occur in the PSTN. VoIP networks can experience “congestion collapse” due to signaling retransmission algorithms and limited overload control capability defined in VoIP protocols. In this situation, the VoIP network’s ability to handle traffic can be reduced substantially below its normal capabilities, and may require a significant amount of time to recover. Industry forums are developing recommendations and guidelines that could minimize this kind of overload.

If the VoIP network is overloaded, the response depends on the nature of the overloaded component(s) and the overload response configured by the provider. The response may also depend on the configuration and design of the networks prior to the VoIP network in the call path. Responses may include:

- The appearance of continued normal call processing, except that calls are not actually established.

[6] See FCC Public Safety and Homeland Security Bureau’s Personal Localized Alerting Network (PLAN) at <http://www2.fcc.gov/pshs/services/plan.html>.

- Tones/announcements advising of network overload.
- Signaling that can be interpreted by preceding networks and user equipment as an overloaded condition.
- The call can be re-routed to an alternate route.

All of the scenarios referenced here could result in the blockage of originating or terminating emergency calls.

8 Differentiated Categories of Auto Dialed Calls

It is first helpful to differentiate between auto dialed calls that are legitimate uses for public safety, calls that are more informational in nature, and those calls that are potential illegal activities, and then assess the risk and impact on the PSTN, ENS, and the ICT industry, as well as consumers. The following matrix provides such illustration.

Table 8. 1 - Robocall Definition Matrix

	Legitimate Uses for Public Safety		Current Business Practices				Potentially Illegal Activities			
Risk & Impacts	**Public Emergency Notification**	**Severe Weather Alerts**	**Political Solicitation**	**Solicitation for Charities**	**School Closing Announcements**	**Informational Surveys**	**Intentional Denial of Service Attack**	**Phishing for Active Subscribers**	**Pumping Calls for LIDB DIPs**	**Focused Nuisance Attack**
Network Congestion	High	High	Medium	Medium	High	Medium	High	Medium	High	Medium
Blocking E911 Calls	High	High	Medium	Medium	High	Medium	High	Medium	High	High
Wasted Employee Time	Medium	Medium	High	High	Medium	Medium	High	High	High	High
Cost to the Industry	Low	Low	Low	Low	Low	Low	Medium	Medium	Medium	Medium

Legend

High: Has high potential of experiencing the risk or impact

Medium: Has medium potential of experiencing the risk or impact

Low: Has low potential of experiencing the risk or impact

Depending on the type of call and the associated risk/impact on the network, calls may need to be prioritized (in the case of Public Emergency Notifications and Severe Weather Alerts), or further investigated should there be potential illegal activities.

8.1 Annoyance Calls

Numerous consumer complaints are registered with telecommunications providers and regulatory bodies related to unwanted robocalls. Consumers are increasingly tired of receiving unwanted robocalls and are looking for more restrictions to add new categories of forbidden type calls to the Do Not Call list. Political calls, calls from companies that consumers do business with, medical calls, etc. are exempt from Federal Do Not Call status. Discussions have occurred at a federal level related to expanding categories in the Do Not Call list and giving consumers more control of the calls they choose to receive.

8.2 Potentially Illegal Type Calls

Since auto dialer equipment is able to generate a relatively large number of calls in a relatively short time, there is the potential for large numbers of violations of regulations associated with the National Do Not Call Registry. In particular, a company may intentionally or inadvertently include numbers from the National Do Not Call Registry (and where the company has not had a business relationship with the called party for at least 18 months) in the set of consumers being contacted. Solutions to this problem parallel the solutions for companies that are not using auto dialer equipment.

In addition, there are calls generated by companies with the intent of pursuing some type of fraud on the consumer answering them. The industry and regulatory bodies are looking for solutions to prevent or minimize these types of illegal or scam calls.

There are possible solutions which can be placed on a consumer line level or switching system or network level that may help mitigate unwanted calls. Many service providers offer blocking or other types of services to consumers to assist in the management of both annoyance and potentially illegal type of calls. Consumers have the ability to purchase or obtain equipment, smartphone applications, or other software to block calls in some instances. On a network or switch level there are potential solutions developed by third parties. When considering a network or switched based solution there are considerations that need to be addressed, such as the following concerns: Should a service provider be making the decisions for the consumers on what calls should be blocked and what calls should go through? Is it possible that a system based solution could be manipulated by learned behavior patterns to block legitimate calls that should go through?

8.3 System Security

Auto dialer equipment itself should be secure so as not to be available for misuse for attack of the network by flooding it with calls. Historically, auto dialer equipment was cumbersome and expensive and only available to commercial operators. As technology advanced, most data processing equipment, such as laptop computers, can be utilized to generate the mass calling. This exasperates network security.

Relevant policies and procedures need to be in place to protect the auto dialer system from such things as external attacks, keeping an intruder from sending false messages to the public, or ensuring that constituents' private information is protected. System and data security is of the utmost importance.

Auto dialer providers should employ full-time security measures, undergo regular external security audits performed by a reputable and independent security firm, and deploy intrusion prevention and detection systems. A highly secure network environment using proven best practices must be utilized hand-in-hand with maintenance, updates, and patching to ensure systems are in the most secure state possible.

For security purposes, data files should be encrypted before they are stored in multiple off-site or on-site locations. The company's business continuity plan must address how encrypted data previously removed from the server(s) will be restored and, if stored in an off-site location, the length of time required to recover data. Data centers that provide appropriate fail over capability should be utilized to ensure up-time.

The use of an on-site or hosted auto dialer system will require the end user to take a more active role in securing access to the system, protecting private data, and ensuring system uptime. This may require ensuring that systems are current and personnel are properly trained.

End users should manage employee access to the system in order to ensure that only appropriate messages are generated.

9 Best Practices for Emergency Notifications [Formerly ATIS-0300113]

9.1 General Information

Paths for message delivery are no longer simple. A variety of means can be used to send messages. With the evolution of technology to send mass communication, best practices are needed to ensure that the integrity of the communications network is being considered. With the rise of mass notifications being sent through next generation technologies, such as VoIP and cloud services, a provider may only require a lead time of hours to set up a notification. This could strain the network.

There are several ways that the ENS connects to the communications network. Some of the options include going through the hosting center, T1, analog (POTS), Voice over IP (VoIP), or other. It is important to know how ENS systems initiate calls in an event. Some send by address or specific location, followed by random telephone number, sequential TN, and prioritized by TN. ENS notifications (can be sent/ or are primarily sent) to phones using wireline, wireless, VoIP, or in some cases via text messages. Other ways to disperse emergency notifications include: cell broadcast, really simple syndication (RSS), community information line, sirens, public address system, emergency alerting system (EAS), pager, fax, local radio broadcast, digital signage, or teletypewriter (TTY).

ENS users generally are not notifying their local ICT service providers when issuing an ENS alert. It is recommended that ENS users should notify ICT service providers prior to or when sending out an ENS alert. This initial notification could be done via: phone call, e-mail, or as one of the first ENS alerts sent out to the local ICT.

A small number of ENS users operate in a state that requires registration or a permit. Most states do not require ENS users to register. Typically ENS users are either uncertain or do not know if their neighbouring communities have a ENS system served out of the same central office as theirs is. ENS users who operate out of the same central office switch system may send out notices at the same time ultimately causing congestion or outages in the network. It may important to know where the originating telephone number for the alert comes from; local central office or ENS provider from some other locality. It is recommended that ENS users should check with neighbouring communities to see if they have ENS systems or if that system is served out of the same central office.

The NGIIF has developed and published ATIS-0300098, *Best Practices for Emergency Notification System (ENS) Call Volume Testing Procedure: Wireline.* It is recommended ENS providers/users test with their local service providers when entering an area and periodically (as locally negotiated) to maintain the integrity of the network. See the document for additional information.

9.1.1 ENS Use

ENS users typically use the system to: notify the public of emergency events, and to notify other pre-established groups such as: parents, teachers, students, staff, employees, responder agencies, SWAT, town board (employees). In some cases they are used to notify officials or media. Frequently, these are life threatening events including weather.

Some event usage of ENS systems have been identified primarily for non-life threatening events such as meeting/event notifications, traffic light outages, hazardous road conditions, fraud alerts, cybercrime , school cancellation announcements. Other noted events include attendance, public events, embedded operations channel (EOC) activation, other government agency events, police investigations, water outages.

In many cases other types of notification systems are also used in an emergency. The largest majority use local media some use National Oceanic Atmospheric Administration (NOAA) weather radios, and some use sirens. ENS users use these other systems in combination with the ENS alert. Other systems being used may include: e-mail, twitter, phone calls, common alerting protocol. Website, text messages, cable TV, paging system, Ham Radios, and EAS.

9.2 ENS Providers & Vendors Working Together

It is recommended that ENS providers work with ICT service providers to optimize the delivery of time-sensitive notifications sent through communications networks. The traditional PSTN telecommunication infrastructure was built to handle a percentage of its customers picking up the telephone simultaneously. While that percentage is determined based upon heavy call volume during normal busy periods, it does not anticipate unusual circumstances, such as a mass notification event, that might cause a significant spike in the number of people attempting to place a phone call than is within normal bounds. During times of emergency, damage that might have occurred to the local telecommunication infrastructure will also have an impact on the network.

Mass notification providers that lack experience working with ICT service providers to balance and throttle calls based upon what the area is likely to be able to handle may unknowingly decrease the capacity available to them and to others when they blast a large number of calls at once. This may delay recipients receiving messages and may inhibit their delivery entirely. Too few telemarketers and mass notification providers proactively work with ICT service providers.

An ENS provider needs to clearly understand and have proven experience and technical expertise delivering a large number of time-sensitive calls within a concentrated area. ENS providers need to understand the importance of delivering time-sensitive notifications, routing calls and navigating network congestion, and best practices relative to usage.

Typically ENS users do not contact their telecommunications providers prior to deploying their systems, do not coordinate, or test their system with their telecommunications service provider. There are operational and capacity need benefits to testing.

9.2.1 Types of Emergency Communication Devices

While this guideline focuses on emergency notifications sent through auto dialers, it is important to understand that there are a variety of communications devices that may be able to receive emergency notifications, such as fax machines, personal digital assistants, cell phones, and computers. It is also possible to “push” emergency notification messages to a targeted area experiencing an emergency through software and targeting specific cell towers. It is important for ENS providers to understand what type of notification to send and the impact of sending the message through that technology on the network.

9.2.2 Wireless Emergency Alerts (WEA)[7]

Wireless Emergency Alerts (WEA), formerly known as the Commercial Mobile Alert System (CMAS) (or Personal Localized Alerting Network (PLAN)), is a public safety system that allows customers who own certain wireless phone models and other enabled mobile devices to receive geographically-targeted, text-like messages alerting them of imminent threats to safety in their area. The technology ensures that emergency alerts will not get stuck in highly congested areas, which can happen with standard mobile voice and texting services. WEA was established pursuant to the Warning, Alert and Response Network (WARN) Act.

WEA enables government officials to target emergency alerts to specific geographic areas (*e.g.*, lower Manhattan) through cell towers. The cell towers broadcast the emergency alerts for reception by WEA-enabled mobile devices.

[7] http://www.fcc.gov/guides/wireless-emergency-alerts-wea

WEA complements the existing EAS which is implemented by the FCC and FEMA at the federal level through broadcasters and other media service providers. WEA and the EAS are part of FEMA's Integrated Public Alert and Warning System (IPAWS).

Wireless companies volunteer to participate in WEA, which is the result of a unique public/private partnership between the FCC, FEMA and the wireless industry to enhance public safety.

Participating wireless carriers were required to deploy WEA by April 7, 2012.

9.2.3 Selecting an ENS Provider to Send Emergency Notifications

It is recommended that users thoroughly vet all ENS providers as they are being considered for sending mass notifications, in the interest of public safety, relative to their experience modifying the delivery rate of messages sent to a particular area. The following areas should be investigated to ensure proper deliver of emergency messages:

- Proof of successfully implementing and testing delivery algorithms together with the ICT service providers (A test protocol is available in ATIS-0300098.)

9.2.4 ENS & ICT Provider Cooperative Testing

ENS and ICT service providers should work together to begin the process of sharing the appropriate information needed to allow for initial and ongoing cooperative testing to adjust systems. A test protocol and best practices are available in ATIS-0300098.

9.3 ENS System Equipment

Emergency notifications can be sent through a variety of methods to a variety of communication technologies. Emergency notification systems can include mass text messaging services or mass automated dialing services. Siren systems, digital signs, or loud speaker (PA) systems are examples of notifying the public at large through a single process. This guideline is focused on emergency notification messages sent to private communications devices, usually requiring collection of individual phone numbers through databases, self-subscription, or by some other method. Emergency notifications can be sent to the public through the following common devices:

- Line-based phones
- Mobile phones
- SMS/Text messages
- Email
- Web posting
- Subscription based instant messages/pop-ups

There are a variety of methods in how these messages can be originated. They can be originated by public safety officials, schools, and local governments, and can cover a variety of situations, such as school closings, weather alerts, or terrorist events. This section focuses on the types of equipment available for sending emergency notifications and best practices associated with using such equipment.

9.3.1 On-site Auto Dialer Equipment & Hosted SaaS Equipment

Emergency notification services can be provided by on-site auto dialer equipment, or hosted off site by an ENS provider, sometimes referred to as a Software as a Service (SaaS) provider. Typically, the system or system equipment is the same independent of whether the equipment is hosted or on-site. The difference is basically who runs and maintains the system, who sends out the alerts, or where the equipment is located. However, it is important to consult with the ENS service or equipment provider regarding compatibility with their telecommunications equipment.

The end user may choose to manage their on-site auto dialer systems themselves or have the equipment hosted at a vendor's location. Typically ENS users optimize their system parameters (e.g., call spacing, traffic flow control, and call rate) for successful maximum call completion. The end user (the city, etc.) will need to dedicate resources to work directly with the ICT service provider to throttle calls and regularly test the algorithms put in place. This is a complicated process and the end user should ensure that they have the resources and the expertise needed.

ENS users can be hosted by a third party, which is frequently coordinated externally outside of their organization. Hosted Systems are managed by an ENS provider or SaaS provider. When hosted by a third party it is common for the ENS user to maintain their own database. There are many companies providing this type of service and each may offer different services and features. The end user choosing a hosted system should ensure that they understand all of the services and features offered.

9.3.2 ENS Equipment Features

End users may desire a service or system with all or some of the following features:

- Includes pre-populated residential and business telephone data that is geocoded and refreshed on a regular basis.
- Includes a mechanism for recipients (the general population that will be receiving messages) to add private numbers/additional numbers and/or means of contacting the individual, language preference, and/or identify other special needs that should be considered when sending messages. There should also be a means to remove oneself from the system. One example of a mechanism may be using an internet interface to add or delete information to desired lists.
- Generates frequent (e.g., nightly), automated updates to contact information stored in any and all databases that might be in use by a particular organization, such as website portals accessible by the public, staff databases, and yellow page or E9-1-1 databases purchased by the organization for the express purpose of sending time-sensitive mass notifications in the interest of public safety.
- Allows public safety users to target recipients in an impacted area quickly and easily, for instance geographical references, to:
  - Reduce unnecessarily notifying a larger population than is needed.
  - Ensure that a Geographic Information System (GIS) expert is not required during a critical period when staffing may be limited.
- Can target recipients via call lists that are:
  - Intuitive for end users.
  - Populated from lists that they have already created in other systems used by the end user dynamically created as needed.
- Provides a level of security before a confidential message is generated.
- Includes brief, single response survey functionality for two-way communication (e.g.,: “Are you currently in a safe location?” or “Do you have food and water supplies?”).
- Provides the option to either send to one primary phone number/contact point for more general communication (to help reduce congestion when a critical event may have reduced available local capacity) or to multiple phone numbers/contact points.
- Provides the ability to control the number of redial attempts.
- System scalability for the ENS provider to increase the size as needed.
- Call throttling capabilities to adjust call rate

9.3.3 Congestion Capabilities

ENS systems may be able to respond to network congestion or unavailability by the following means: retries, call throttling capabilities to adjust call rate, delay of paging, use multiple sites to handle congestion, etc. A few ENS systems may be capable of recognizing network indicators such as SIT, or other standard CO/network indicators, such as: busy, operator intercept, fax, TTY, answer, answering machine.

9.3.4 Disaster Recovery & Business Continuity Procedures

ENS providers should have a disaster recovery and business continuity plan in place. Any single point of failure may result in public safety officials not being able to deliver messages to their constituents. At a minimum, systems should be housed in data centers with appropriate fail over capability. Multiple call origination sites may be beneficial. Multiple delivery paths may be beneficial, such as via email and other technologies currently in use and/or in development (such as those addressed by WEA).

Some notification vendors offer Quality of Service (QoS) and Service Level Agreement (SLA), provide a backup and/or alternate alert initiation process. Back up services provided are typically: customer service, followed by back up site, then automated attendant, and a shared cooperative arrangement with another client or same vendor. Other alternatives were: web based emergency management staff, etc.

ENS providers should ensure that they have the following redundancy recommendations:

- Systems
    - In different geographic location(s)
- Customer support centers
    - In different geographic location(s)
    - Communication capabilities from and to different sources

9.3.5 System Security

Relevant policies and procedures need to be in place to protect the system from such things as external attacks, keeping an intruder from sending false messages to the public, or ensuring that constituents' private information is protected. System and data security is of the utmost importance.

ENS providers should employ full-time security measures, undergo regular external security audits performed by a reputable and independent security firm, and deploy intrusion prevention and detection systems. A highly secure network environment using proven best practices must be utilized hand-in-hand with maintenance, updates, and patching to ensure systems are in the most secure state possible.

For security purposes, data should be encrypted before it is stored in multiple off-site locations. The company's business continuity plan must address how encrypted data previously removed from the server(s) will be restored and, if stored in an off-site location, the length of time required to recover data. Data centers that provide appropriate fail over capability should be utilized to ensure up-time.

The use of an on-site or hosted auto dialer system will require the end user to take a more active role in securing access to the system, protecting private data, and ensuring system uptime. This may require ensuring that systems are current and personnel are properly trained.

ENS users should take security steps to avoid unauthorized use of their ENS systems. The majority of users address security issues against unauthorized use of the ENS. However, there are still too many that don't and security recommendations to do so should be addressed. Most users attempt to protect registered user privacy; however, there is too many who do not. End users should manage employee access to the system in order to ensure that only appropriate messages are generated. (See also Section on 9.3.7 Administrative Access Rights).

9.3.6 Open Platforms/the Ability to Expand System Interoperability

Public safety officials should consider working with communication providers including their mass notification provider(s) that have chosen to take an open approach to contact and messaging APIs. These programming interfaces open up application to application interoperability giving public safety officials' time-saving and data accuracy capabilities critical in time-sensitive notification situations. Such practice should better ensure that alternative and complementary notification methods (such as sirens, visual displays, hotlines, etc.) are utilized in a consistent and immediate manner. The service provider can determine availability and usage of APIs.

9.3.7 Administrative Access Rights

The system should be configured to allow access to certain types of contacts and reports based upon the user's oversight rights. For instance, the mayor or designated person should be able to call all residents, businesses and staff, but the mayor/designated person may choose to allow the head of the department of health and human services to have access to a select subsection of the government entity's staff and, say, all municipal health facilities.

Ensure the service provider has a tool that allows one to modify access rights at the individual level so that they can specify user roles and rights based upon their individual organizational structure. Public safety officials may also want to require the ability to automatically interface with the organization's employee database to ensure seamless, real-time access privileges.

End users should manage employee access to the system in order to ensure that only appropriate system modifications and/or messages are generated. Managing system access rights aids in the protection of the network by preventing usage to send unauthorized mass alerts.

9.3.8 ADA Compliance

Ensure that the service provider can allow the purchaser to remain ADA compliant. Providers should be able to offer a Voluntary Product Accessibility Template (VPAT)[8] that addresses both users (message initiators) and recipients (citizens and residents).

9.3.9 Outbound Caller ID

Vendors should be required to design their systems to comply with FCC 11-161 Paragraph 704 to display the phone number associated with the calling party originating the mass notification message, rather than a generic number or the number from which the recorder is placing the call. It is not advisable that the system display a generic number such as 4-1-1, 9-1-1, or a random vendor-specified number that will not be recognizable by the recipient or allow the recipient to reach a credible spokesperson or recording should they wish to get additional information or have their phone number removed from the system.

End users originating the message should be required to display the phone number associated with the calling party originating the mass notification message, and not populate the field with items such as 000-000-0000 or 999-999-9999. An ENS user should know if their outbound Caller ID is dynamically configurable. It should also be known if their Caller ID number could be used by the recipient to call back for additional information. The consumer receiving the mass notification alert may want to contact the originator of the mass notification for more details and will need a dialable number recognizable to the called party to do so.

9.3.10 Technical Support Access

Users should have immediate access to technical support 24/7.

Regardless of whether one has SaaS or their own equipment, users should have a clear understanding of procedures that they should follow to report, document, confirm a fix, and close an issue.

Require that customer service representatives, technical developers, and data integration specialists have a thorough understanding of emergency issues and that staff is proactively trained. If one is using a mass notification service provider, support representatives should have access to information relative to the particular user's account only after an approved user name and password has been supplied. All support staff should have a clear understanding of the organization's procedures and should have ample knowledge of time-sensitive notification best practices.

9.3.11 Higher Level & Long-Term Support, Including Usage Guidelines

Ideally, public safety officials should be able to benefit from their mass notification vendor providers' expertise. This expertise should transcend how to avoid local telecommunication congestion. The provider should work with its public safety clients to identify how the service fits within the client's overall communication plans as well as assist public safety officials to work with their local telecommunication provider(s) and the public utilities commission to become more familiar with the rules and regulations governing communication in the client's respective area.

[8] The VPAT form is available at the US Department of State, Information Resource Management Program for Accessible Computer/Communication Technology, http://www.state.gov/m/irm/impact/126343.htm

The mass notification provider may also assist its public safety clients to help identify goals common among its other clients and provide reports that track to the goals of the program. Further, the provider should assist public safety officials to understand the policies and practices that they might consider based upon guidelines developed by other clients and/or based upon actual usage of the system by other clients of similar size and/or geography. Alternatively, the mass notification provider may facilitate a discussion among clients with similar needs. Areas of discussion could include script development, department oversight, testing protocol, the appropriate credible spokespeople to deliver certain types of messages, message approval, message prioritization, alternate methods of message dissemination, etc.

Mass notification providers who have tested with their local telecommunication service providers/ICTs will have developed and shared contact information between each other. ICTs and notification providers will work cooperatively to prevent network overloads and/or disruptions. An on-going relationship between parties will assist in the management of time, duration, and quantity of calls safely traversing the network.

Proactive, long-term care and an ongoing dialog between the mass notification provider, the client, and the local telecommunication service provider will encourage a more successful and sustainable program.

9.4 ENS Administration Information

9.4.1 Outgoing Alert System Information

ENS users may be uncertain of the number of attempts made to connect to a call which can range typically from one to five attempts. The most common criteria to warrant a reattempt is: busy signal, ring no answer, network busy, number out of service or disconnected number, answering machine, fax machine, screening services, or follow me/find me.

Many systems detect and react to answering machines, voicemail systems; however, it is not as clear when it comes to screening services. Typically systems do not duplicate numbers and do not appear to have an option for call recipients to transfer to a live operator. Many messages will include a telephone number the recipient may call for more information (which is determined locally).

The typical duration of the total message, including call set up, call take down, and, where applicable, replays and outgoing answering machine messages is 60 seconds, followed by 45, 30, and sometimes 15 seconds.

9.4.2 Performance

The majority of ENSs can monitor performance; however, they may differ in the ability to calibrate the system in real time or not.

Typically ENS users do not prioritize simultaneous notifications which may impact performance ability. ENS users who do prioritize simultaneous notifications may prioritize on the following example or use some other methodology:

1. Based on severity or impact to life, limb or property
2. Through pre-approved policy
3. First come first served
4. Size of impacted group

9.4.3 Sources & Management of Database Contact Information

ENS databases are populated with phone numbers obtained from a variety of sources. ENS databases need to accommodate phone numbers, fax numbers, e-mail addresses, or SMS numbers which could range anywhere from 0 to an unknown number.

Public safety officials should consider the type of data available to them, the cost, and the ability to update that data. Some mass notification vendors include publicly available resident and business telephone numbers with their systems. E9-1-1 data may be available from the local telecommunications provider. In some cases E9-1-1 data lists have requirements where that data should only be used for emergency situations.[9]

The ENS contact information should be verified both when entered into the database and periodically after that to determine whether the number has been disconnected or moved. Public safety officials should clearly understand how frequently that data is updated to ensure that outdated contact information is not further contributing to network congestion each time a call is placed. Some ENS providers have the ENS users manage their databases and phone lines, while other users manage their hardware and data network.

When possible, contact information should have geocodes appended so that public safety officials can target message recipients based upon their location which will reduce the number of recipients being unnecessarily contacted as well as better ensure that telephone network congestion is managed.

Finally, a means for the public to enroll and/or delist themselves from the service should be included. Public officials may also need to supply the public with a means of including special instructions about their language preference, special communication needs, additional contact points, etc.

9.4.4 Targeted Geographic Recipients

If end users wish to target specific recipients in a particular geography, then they need to ensure that their vendor has mapping capability to do so. Vendors, or other sources, may be able to supply a robust mapping tool that will allow users to draw points on a map to target recipients based upon their geocoded location. The end user should ensure that the vendor is supplying data with geocodes appended and data is updated on a regular basis.

9.4.5 Special Groups & Call Lists

Users should be allowed to create an unlimited number of call lists (groups and sub-groups) within their individual accounts. Public safety officials may also wish to require the service to automatically pre-populate groups and sub-groups that are intuitive to its users based upon an automated, unattended feed from other services/systems used.

9.4.6 Updating/Modifying Existing Recipient’s Registration Information

Some public safety officials may have created their own databases for emergency notifications based on available data from various sources. Others may allow recipients to individually register to receive emergency notifications. In both cases, public safety officials should ensure that recipients are able to add/delete/modify their registration information for emergency notifications. Public safety officials should consider creating a simple online data collection form that allows the recipient to determine preferences during the initial registration process, such as the ability to opt-in or opt-out of mailings or certain types of non-emergent notifications. Public safety officials may initially or periodically use these emergency notification lists to notify recipients via mail stuffers in utility bills, with tax statements, and/or in a separate mailing that they can update their information.

9.4.7 Native Language & Data Collection

The system should automatically extract from the database provided the native home language spoken and/or include a mechanism by which the recipient can identify their preferred language. When a user elects to record and send a message in a language other than English, he/she simply selects the appropriate language, records the message in that language and the system automatically targets just that section of the database. Some providers include translation services or automatic computerized translation; however, caution should be exercised by the user sending the message that the translation is accurate as slang can be an issue for even the best translation packages.

[9] It should be noted the term ‘emergency’ may differ among different users. An emergency to one entity may not be classified as an emergency by another.

9.4.8 Data Integration

Data should be transmitted securely. A secured connection and process is required (e.g., e-mail does not provide adequate security for personally identifiable information). One should confirm with references that the data transfer process was performed as described by the vendor.

9.4.9 Recording & Personalizing Messages

Some vendors have text-only services removing the power of delivering messages in the user's own voice. This may cause recipients to reach out to others to confirm the validity of the message, further increasing congestion on the local telecommunication infrastructure as well as delaying the recipient from taking the appropriate action.

As an example, some mass notification providers allow users to send a message recorded in a credible spokesperson's own voice and then include personalized data specific to the message recipient (e.g., street name, person's name, or zip code) using text-to-speech functionality. Some public officials may find that this blended approach is a beneficial way to get pertinent information to recipients (for instance, about a particular time that they should evacuate based upon the area in which they reside) while better ensuring that the public recognizes the validity of the message being delivered.

9.4.10 Preloaded Scripts

It is beneficial to include pre-approved personalized scripts in the system that map to the emergency operations plan so that end users have immediate access to information applicable to key events. Some mass notification providers may have sample scripts available; however, public safety officials should consider requiring the vendor to load personalized scripts into the system. Public safety officials should also consider having scripts translated into the languages applicable to the area/database of constituents.

9.4.11 Ability for Recipient Access to Previous Messages

Public safety officials should consider the inclusion of a toll free number that constituents can call to retrieve messages sent to them previously. This may be a feature provided by the mass notification provider. Some mass notification providers include additional security functionality that limits message retrieval to those calling from the phone number to which the original message was sent.

Officials may also wish to have a general line where standard messages (approved for anyone to hear) can be accessed or they may wish to integrate a 311 service into the mass notification process.

9.4.12 Lost Passwords & Support

If you are using a SaaS provider, consider requiring the SaaS provider to handle all support issues, such as lost passwords. Ensure that the provider has 24/7 support and that all officials with rights to place a call have the ability to contact the provider directly.

If one has purchased and is maintaining its own auto dialer equipment, consideration should be given to how these issues will be resolved on a 24/7 basis.

The goal is to ensure that calls can be placed as quickly as possible and that the organization does not introduce a single point of failure (for instance, if an employee is on vacation) should a problem arise.

9.4.13 Call Reports

Most systems are capable of receiving reports identifying success/fail rates, percentage of successful notifications by time after the notification began, response rates to touchtone survey, number of calls to the callback number if provided, system downtime availability, and call results for a particular phone number. Typically reports are not generated as events are occurring, and many systems do not get reports until after the event has concluded.

ENS users should determine what types of call reports (standard or custom) are available to them through their system. Reports should be made available immediately upon call completion of the mass notification event. Aggregate information should be supplied (quantity reached live, by answering machine, quantity of invalid numbers, fax machines, etc.). In the interest of security, reports should not include personally identifiable information. Reports with personally identifiable information should only be provided after an ENS user logs in to their password protected account.

10 Conclusion

Telephone networks are not designed to support large volumes of community alerting calls to one area in a short time frame. This is true regardless of the technology used by the phone network; whether it is the PSTN, VoIP, or cellular/wireless.

Annex A: Type of Auto Dialers & Definitions

(informative)

This attachment identifies representative examples of different types of auto dialers, how they are used, or what they are called. This list is not all inclusive and has been gathered from a variety of sources. There may be other definitions available. Terminology and definitions may somewhat overlap since all are variations of the generic aspects of auto dialers, reflect technical and lay terms which have evolved over time, reflect lack of standards in regards to auto dialer terminology, may reflect the function of an auto dialer.

Automated Notifications

Proactive calls intended to provide the recipient with important information, such as a local township's tornado warning notice, an airline's flight-delay or seat upgrade notification, a healthcare provider's reminder of an impending appointment, etc. Automated notifications are typically authorized or wanted by the called parties.

Auto Dialers (generic)

An auto dialer as defined in this document, sometimes called an Automatic Calling Unit, is an electronic device that can automatically dial telephone numbers to communicate between any two points in the telephone, mobile phone, and/or pager networks. Once the call is established (through the telephone exchange), the auto dialer can connect with a live agent, provide a prerecorded message, or transmit digital data (like Short Message Service (SMS) messages) to the called party.

When an auto dialer plays a pre-recorded message, it is often called "voice broadcasting", or "robocalling". Robocalls are the results (pre-recorded messages) of a call placed via an auto dialer. Some robocalls ask the person answering to press a button on their phone keypad, such as in opinion polls in which recipients are asked to press various digits in response to questions asked by the message. These types of calls are often called outbound Interactive Voice Response (IVR).

There are different types of Auto Dialers: Smart Auto Dialer, Semi-automatic Dialer, Distributed Dialers, Predictive Dialers, as well as others defined in this attachment.

In addition to PSTN capabilities, auto dialers may also have VoIP capability.

Distributed Dialers

Some enterprise grade auto dialers are distributed dialers, i.e., independent dialers that are linked together through the Internet and controlled by a call dispatching program. With distributed computing, there is virtually no limit on scalability. All distributed dialers, by definition, can be accessed remotely. Today with optimized and highly specialized coding some companies have been able to sustain 2000 simultaneous calls using only one server and a single 100 megabit connection.

Hardware Dialers

Hardware dialers use dedicated telephony boards to perform call progress analysis and answering machine detection. Those switches usually have two main types of connections: agent audio and external audio.

The agent audio connections are usually simple T1/E1/ISDN etc. telephony spans that are connected directly to an existing PBX (although other connection types that do not require a PBX are available such as Analog or VoIP connections). When an agent logs in, the dialer will place a call from the switch directly to the phone on the agent's desk. This open phone call between the agent and the dialer switch is then kept open for the duration of the session.

The second type of connection is the external audio connection used to make outbound phone calls. These connections are typically ISDN/T1/E1 connections direct to the PSTN. When an outbound call is made and answered, the call is immediately joined to an already open agent audio connection of the agent selected to take the call.

NOTE: Fewer telephony connections may be required (In hard dialers external audio connections can go directly to the PSTN). Dialer typically will not need upgrading in line with PBX/CTI etc.; since standard telephony connections are the only link between the PBX and the dialer, the dialer is less affected by software changes/versions. Capacity for handling calls may be up to 100,000 calls per hour.

Hosted Predictive Dialers

Hosted predictive dialers (aka Virtual Predictive Dialers, Web-Enabled Predictive Dialers, VoIP Predictive Dialers) use the Software as a Service (SaaS) model to provide predictive dialer capability. Typically, the only requirement to use a hosted predictive dialer system is a computer with an Internet connection and a telephone line for each agent. Links into the system are remote, enabling agents and supervisors to connect from any location.

NOTE: Service is dependent on an Internet connection; when the Internet goes down, so does the service provider using VoIP as its primary delivery method experience limited reliability and performance. Often, far more limited in capability than an "On Site" product.

Hybrid Predictive Dialers

Hybrid predictive dialers are soft dialers that rely on a hosted VoIP service for calls. Unlike soft dialers, a hybrid dialer does not connect to an existing PBX system. Instead, it connects to a VoIP service provider through Internet connections.

NOTE: May have lower call-processing capacity. Service is dependent on an Internet connection; when the Internet goes down, so does the service.

Predictive Dialer

When an auto dialer connects an answered call to a live agent, it is often called a predictive dialer or power dialer and uses real-time analysis to determine the optimal time to dial more numbers. A power dialer simply dials a pre-set number of lines when an agent finishes the previous call.

A predictive dialer dials a list of telephone numbers and connects answered dials to people making calls, often referred to as agents.

For Emergency Notification purposes, use of an agent versus pre-recorded announcements should be considered.

If someone answers but no agent is available within two (2) seconds of the person's greeting, FCC regulations consider the call "abandoned" and require the dialer to play a recorded message. The FCC requires that predictive dialers abandon less than 3% of answered calls.

A “silent call” is a call generated by a predictive dialer that does not have an agent immediately available to handle the call. In this instance, the call may be terminated by the dialer, and the called party receives a silence (“dead air”) or a tone from the telephone company indicating the call has been dropped.

In the United States, the Federal Trade Commission (FTC) uses the term "abandoned call" instead of “silent call” in its regulations applying to telemarketing. Abandoned calls in non-FTC contexts may refer to a caller who decides not to await answer before hanging up.

Semi-Automatic Dialer

A semi-automatic dialer is a human controlled dialer. All actions, such as dialing, playing audio message, recording, are initiated by human, normally by the press of a key. It is a productivity tool for telemarketing agents.

Smart Auto Dialer

A smart auto dialer is an auto dialer capable of personalizing messages and collecting touch tone or speech feedbacks. A speech engine is usually included for converting text to speech and recognizing speech over the phone.

To customize or personalize messages, a smart auto dialer system uses message template, which contains variables that can be replaced later by actual values. For example, a time variable included in the message template can be replaced by the actual time when a phone call is made.

Smart Predictive Dialers

Smart predictive dialers combine auto dialer function with voice messaging and phone agents who are prepared to handle calls initiated by the dialer. Answering machines, busy signals, and unanswered calls are processed in a manner similar to that of a normal predictive dialing system. However, when a 'live' answer is detected, the dialer plays an introductory recorded message, giving the call recipient the option to talk with an agent to complete the transaction. This message is a consistent greeting that identifies the caller, the nature of the call, and the option to speak with an agent. This process requires a more sophisticated predictive algorithm to ensure that a phone agent is available when the call recipient asks to speak with an agent.

> NOTE: Certain U.S. states do not allow recorded messaging (unless prior business relationship has been established). This may limit the use of this technique to only certain types of business or consumer campaigns in certain geographical areas.

Soft Dialers/Software-only Dialers

Software-only dialers are often cheaper because they do not require expensive telephony components. Utilizing the ever increasing computational power and shorter development cycle, today's soft dialers offer the same or more functionalities than traditional hardware based dialers. For example, call progress analysis and 'call classification' are all implemented in the software. In addition, it is usually easier to integrate other 'voice' related functions (voice recording, IVR, speech recognition, text-to-speech etc.). Typically, a software dialer is connected to an existing PBX system via the PBX CTI link. Open Source dialers have proven themselves in the production world and enable call centers of all sizes to lower costs. Other advantages include customization of the software suites to meet the needs on an individual basis.

Recent soft dialers are mostly VoIP dialers. These dialers can connect to VoIP compatible PBX systems the same way as traditional software dialers. In addition, VoIP dialers can connect to VoIP services directly through the internet.

Older soft dialers may use ISDN messaging, or a CTI link to provide call progress analysis for calls made, and in some cases, specialized 'call classification' cards are required in the PBX for call progress analysis and answering machine detection.

Pros:

- Low cost without consideration of sunk costs of a fully-provisioned PBX
- Flexible architecture works well in multi-site and distributed environments

Cons:

- A few older PBXs will not work with a soft dialer configuration
- Older dialers have higher error rates in classification of calls (fax, modem, etc. have to be detected by the agent)

Telemarketing Dialer

An enterprise grade dialer must provide two key features. First, it must be capable of making large number of simultaneous phone calls; and second, it must provide an Application Programming Interface (API) for system integration. Almost all enterprise grade auto dialers employ computer networking technology, since voice boards have fixed number of ports and cannot be scaled up. In order to make 2000 simultaneous phone calls, for example, a group of computers have to be linked together to provide the support for that many phone lines.

Tele-Town Hall™ Dialer

A Tele-Town Hall™ dialer is a program used by individuals, such as public officials, to a conduct a large scale telephone conference call with constituents. When a Tele-Town Hall™ meeting is established, the auto dialer will call a group of phone numbers that has been identified by a method such as zip code or actual telephone number. The recipient of the call will usually have the option to either participate in the call or hang up.

War Dialer

A war dialer is a computer program used to identify the phone numbers that can successfully make a connection with a computer modem. The program automatically dials a defined range of phone numbers and logs and enters in a database those numbers that successfully connect to the modem. Some programs can also identify the particular operating system running in the computer and may also conduct automated penetration testing. In such cases, the war dialer runs through a predetermined list of common user names and passwords in an attempt to gain access to the system.

WarVOX

WarVOX is a free, open-source war dialing tool for exploring, classifying, and auditing telephone systems. WarVOX processes the raw audio from each call and does not use a modem directly. WarVOX finds and classifies telephone lines using signal processing techniques. WarVOX uses Internet-based VoIP providers instead of the typical telephony hardware used by traditional war dialers. By comparing the pauses between words, WarVOX can help pick out numbers that used the same voicemail system.