

Appendix A

This appendix provides a list of AT&T's capabilities across the wireline, Uverse and wireless portfolio that support

- Call Blocking (Black list)
- Call Screening
 - Call ID
 - White List
- Do Not Disturb
- Call Tracing

Summary for Wireline

- Call Block / Call Screen
 - Fee Based
 - 10 number block capacity
- Privacy Manager
 - Forces anonymous, unavailable, out-of-area, and private to identify themselves before call completes
- Anonymous Call Rejection/Blocking
 - Callers are told to hang up, unblock delivery of their caller ID and call back.
- Call Trace
 - Allows the harassing, threatening, or annoyance call to be traced

Summary for U-Verse

- Call Blocking
 - 20 numbers can be blocked
- Anonymous Call Blocking
- Call Screening
 - 20 numbers can ring through while all others blocked
- Do Not Disturb
 - All calls blocked
- Call Trace
 - Allows the harassing, threatening, or annoyance call to be traced

Summary for Wireless

- Smart Limits
 - Block data and up to 30 numbers from text and calls
 - Time Restrictions –
 - Limit texting, outbound calls & cellular data use during specific times
 - Text Limits - Set sensible limits on the number of texts sent and received
 - Purchase Limits- Limit purchases for apps, music and games billed to your AT&T account

Summary for AT&T Business

- Wireline
 - IPFlex (SIP [Session Internet Protocol] offering)
 - Call Screening (white list)
 - Time of Day Blocking
 - Call Blocking – Specific Numbers or Pattern Matching
 - Do Not Disturb
 - Anonymous Call Blocking
 - Special Note → Available wherever AT&T sells AVPN (AT&T Virtual Private Network), EVPN Enhanced Virtual Private Network) and MIS (Managed Internet Service)
 - All-in-One Call Screening
 - Anonymous Call Rejection
 - Call Blocking
 - Selective Call Rejection
 - Distinctive Ring
 - Local / Long Distance
 - Call Blocking for up to 10 specific numbers
 - Ring Central
 - This is a 3rd party product resold by AT&T
 - As a cloud based PBX, this product has a robust set of capabilities.

Details on U-Verse

Name of Capability	Web	General Description	Limitations	Availability
Call Blocking (Black List)	Link	Consumers can block up to 20 numbers. The 20 numbers are loaded online. After loading the 20 numbers, call blocking (black list) can be turned on and off through the online portal or from the phone.	Call Blocking and Call Screening can't be active at the same time	21 State Footprint ¹
Anonymous Call Blocking	Link	Anonymous Call Blocking helps you avoid unwanted calls from anyone whose caller ID information is blocked. Your phone does not ring and the caller is unable to leave a voice mail message. Callers who have their caller ID information blocked will hear, "The number you dialed does not accept calls without caller ID information." This can be turned on an off in the online portal or directly with a customer's phone.	Call Blocking and Call Screening can't be active at the same time	21 State Footprint
Call Screening	Link	Call Screening allows calls to ring through from a list of up to 20 phone numbers specified by you. If someone calls you from a number not on your list, the caller will hear, "The number you dialed will not accept your call." The call will end, and the caller will not be able to leave a message. Setup your call screening list online and edit as often as you wish. You can turn call screening on and off from the portal and the phone.	Call Blocking and Call Screening can't be active at the same time	21 State Footprint
Do Not Disturb	Link	The Do Not Disturb feature gives you the option to turn off the ringer on your home phone. When the service is activated, callers will hear a busy signal. To activate by phone, dial *78# on your home phone. To deactivate, dial *79#. You can turn do not disturb on and off from your portal or your phone.		21 State Footprint

¹ Service is available only in U-Verse coverage area in 21 state footprint.

Appendix A

Call Trace	Link	Immediately after you receive an annoying or harassing call, pick up the phone and dial *57. Follow the recorded instructions to invoke this Call Trace feature - automatically tracing the last call you received. You are responsible for filing a complaint with the law enforcement agency. After three successful traces, we will release the call origination number to the law		21 State Foot-print
------------	----------------------	---	--	---------------------

Details for Wireline

Name of Capability	Web	General Description	Limitations	Availability
Call Block/Call Screen	Link	Call Block/Call Screening is a feature that is available at a low monthly rate. With Call Screening you can block up to 10 phone numbers within your local calling area. You can also block the last incoming call received, even if the number is unknown (e.g., block solicitation calls). The blocked caller hears the message: We are sorry, the party you're calling is not accepting calls at this time.	All 10-digits of the number, including the area code, are needed when adding a number. Some cellular numbers cannot be blocked. 800 numbers cannot be blocked. This service is not available in all areas.	21 State Footprint ²
Privacy Manager	Link	Privacy Manager is a call screening service that works with Caller ID to identify all incoming calls that have no telephone numbers provided and which are identified as Anonymous, Unavailable, Out-of-Area, or Private, and requires callers to identify themselves in order to complete the call. You'll know who's calling and have four options for handling the call. You also have the option to provide frequent callers whose numbers are unidentified, with an access code/PIN feature which will allow them to ring through to your phone without recording their name (Profile Manager).	Profile Manager not available in MW Region	21 State Footprint
Anonymous Call Rejection/Blocking	Link	Anonymous Call Rejection (ACR) /Blocking or ACR intercepts calls from people who have used a blocking feature to prevent their name or number from being provided to people they call. When the ACR service is activated, callers hear a message telling them to hang up, unblock delivery of their phone number and call again. Your phone will not ring unless the caller removes the block.	ACR stays on until you turn it off. If a call comes in from a private number on your Personalized Ring or Selective Call Forwarding list, the call will be accepted. ACR does not block Operator Assisted incoming calls. Caller ID is required in some areas. Does not intercept calls that display as Unknown or Out-of-Area on the Caller ID. These designations usually mean that the call originated in an	21 State Footprint

² Services listed are in the legacy coverage areas of our 21 state footprint.

Appendix A

			area in which Caller ID is not available.	
Call Trace	Link	<p>Call Trace helps to handle obscene, harassing or threatening calls. This feature should only be used to trace harassing or threatening calls that warrant legal action. Successful trace information is provided only to the customer's law enforcement agency and will be used when investigating harassment. Call trace information is never divulged to the customer by AT&T.</p> <p>Call Trace allows customer to initiate an automatic trace of the last incoming call received. Customer must dial designated code to activate the option each time want to trace the last call. Call Trace is a pay-per-use option.</p>	This option is not available in all areas. All Regions have Call Trace as a pay per use feature; Call Trace is also available as a feature in SE Region.	21 State Footprint

Details for Wireless

<i>Name of Capability</i>	<i>Web</i>	<i>General Description</i>	<i>Limitations</i>	<i>Availability</i>
AT&T Smart Limits SM	Link	<p>Set Blocks:</p> <ul style="list-style-type: none"> - Block Data - block access to cellular data - Block Numbers - block up to '30' numbers from unwanted calls and texts including 411. <p>Set Limits:</p> <ul style="list-style-type: none"> - Time Restrictions - Limit texting, outbound calling and cellular data use during specific times - Text Limits - Set sensible limits on the number of texts your child sends and receives - Purchase Limits- Limit purchases for apps, music and games billed to your AT&T account <p>View Activity:</p> <ul style="list-style-type: none"> - Daily Activity – Check your family’s phone activity with texting and calling activity graphs - Weekly Reports - Receive weekly reports summarizing texting and calling activity - Alerts - Get customized alerts for text and call activity and receive new contact alerts - Top Contacts - stay in touch by knowing who and how often your child is communicating with Contacts. (Accessible from web and Android app. Not accessible through the app on iPhone at this time.) 	<p>Compatible phone w/eligible. data plan req'd. Data & messaging rates may apply for app download & usage.</p> <p>Blocks: blocked numbers blocks 10 digit U.S. phone numbers with valid area codes and calls to 411. May not block other 10 digit numbers like international numbers. Blocked numbers does not block picture/video messaging and/or 3rd party messaging services. Data blocks apply to cellular data usage only. Does not block Wi-Fi usage. Time Restrictions: are not guaranteed to be precise. Incoming calls allowed at all times including during time restrictions, except from numbers designated as “Blocked Numbers.” General: Technical, network and other service limitations may apply. Coverage not available everywhere. Intended for US service only. App may use personal info. This use governed by AT&T's Privacy Policy found at att.com/privacy.</p>	Coverage not available everywhere. Intended for US service only.
Individual Mobile Devices	Link	In addition, many wireless devices offer the capability to block unlimited calls and messages free-of-charge through the device settings. AT&T’s Device How-To Center provides consumers information on device capabilities and instructions for blocking calls and texts.		The device capabilities are available even when roaming Internationally.

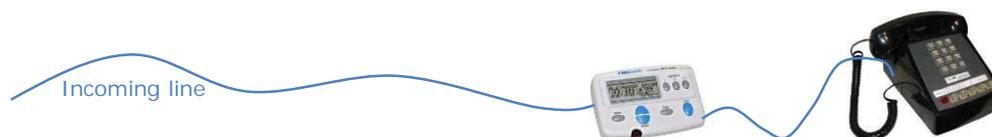
Details for Business Wireline

Name of Capability	Web	General Description	Limitations	Availability
IPFlex (Internet Protocol Flexible Reach)	link	<p>IPFlex Call Screening</p> <ul style="list-style-type: none"> • Anonymous call blocking • Call Acceptance (whitelist capability) <ul style="list-style-type: none"> o Accept calls from any number o Accept calls only from specific numbers <p>Wildcards are available. You can use a “?” for a single position or an “*”</p> <ul style="list-style-type: none"> • ?52* would accept any number that had 52 in the 2nd and 3rd position • 8* would accept any number starting with 8 <ul style="list-style-type: none"> • Schedule time of day blocking • Reject calls from any number • Reject calls from specific phone numbers (Blacklist capability) <ul style="list-style-type: none"> o Wildcards are available. You can use a “?” for a single position or an “*” § ?52* would reject any number that had 52 in the 2nd and 3rd position § 8* would reject any number starting with 8 	Outside of incumbent coverage area, AVPN, EVPN, and MIS would have to go through a local incumbent carrier.	Coverage area in 22 State Footprint. Plus Coverage is available across all 50 states when used with EVPN, AVPN, and MIS
All-In-One Call Screening	Link	AT&T All In One Call Screening Features (target for Small and Medium Businesses(SMB) Anonymous Call Rejection, Caller Blocking, Selective Call Rejection, Distinctive Ring		21 State Footprint
Local/Long Distance	Link	Caller ID with Name and Number See the caller's name and number displayed. Call Screening prevents you from receiving unwanted calls from up to 10 specific numbers within your service area.		
Ring Central	Link	RingCentral is a cloud based VoIP PBX sold by AT&T. You can block callers, provide time of day blocking, provide time of day routing to voicemail, require a caller without caller ID to say their name, refuse pay phone calls, set do not disturb,		

Appendix B

This appendix contains a technology survey of 3rd party products and provides a summary of capabilities and cost ranges. There are thousands of 3rd party products and services. This survey is a sample of the 3rd party vendors. Samples are across the following four categories:

1. Inline – telephone line to the device and then to phone



2. Phone/Device



Device has capabilities built-in

e.g. Panasonic Dect 6.0 phone can black/white list

3. Service



Call is transferred to "sas" where it is screened. If approved, call is then sent to home phone. This service is configured via the web and requires the call transfer capability *72 and *73



Call has simultaneous ring at Nomorobo site and home. If number is on Nomorobo's list of fraudulent calls, call is terminated at Nomorobo site. Requires the ability to have simultaneous ring. Configure at nomorobo.com.

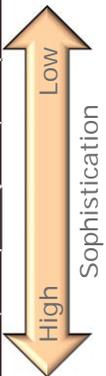
4. Wireless

- Smartphones
- Apps (applications on smart phones)

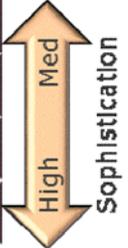
3rd Party Summary

The black circle is an indicator of whether the solution complete supports a feature. For instance, Telezapper gives a “disconnected” tone to the caller to fool computer calling systems to believe the phone is disconnected and removed the number from their database. This product will still allow calls. If the robocaller doesn’t remove the number from their database, the call could still reoccur.

3 rd Party Device	Price Range	Call Block Blacklist	Text Block Blacklist	Call Screen White List	Text Screen White List	Reject Anonymous	Do Not Disturb
Caller ID	\$20 to \$50						
Robo Defeaters e.g. Telezapper*	\$25 to \$35	●					
Call Blocker with Manual Touch	\$40 to \$60	●					
Call Blocker with Larger Display	\$60 to \$90	●					
Call Blocker with Capabilities	\$40 to \$60	●		●			
Call Blocker with Most Capabilities	\$50 to \$120	●		●		●	●



3 rd Party Phone	Price Range	Call Block Blacklist	Text Block Blacklist	Call Screen White List	Text Screen White List	Reject Anonymous	Do Not Disturb
Home Phone Basic Functionality	\$50 to \$80	●					
Home Phone Rej /DND Func.	\$60 to \$90	●				●	●
Home Phone Advanced	\$90 Plus	●		●		●	●
Advanced Phone With Bluetooth*	\$120 Plus	●	●	●	●	●	●



Web Service	Price Range	Call Block Blacklist	Text Block Blacklist	Call Screen White List	Text Screen White List	Reject Anonymous	Do Not Disturb
Web Based and Call Forwarding	Free- To Per Call	●	●	●	●	●	●

3 rd Party Provided	Price Range	Call Block Blacklist	Text Block Blacklist	Call Screen White List	Text Screen White List	Reject Anonymous	Do Not Disturb
Smartphones*	Free – in device	●	●			●	●
Apps – e.g. iOS & Android	Free to \$10	●	●	●	●	●	●
Wireless Carrier Services**	\$5 to \$10 recurring	●	●	●	●	●	●

Appendix C

This appendix contains a list of initiatives outside of AT&T

Summary



Study group on security and spoofed caller ID



Voice & Telephone Working Groups
Published documents and Guidelines



Stage 2 of Study on Spoofed Call Detection / Prevention
Security Working Group active with specification FS_SPOOF



Conducting workshops and seminars on Caller ID Spoofing
Embracing IETF Efforts and Standards



Several members are creating white papers on caller ID
blocking and spoofing.
Some members have implemented caller secure ID.



ATIS-NGIIF has 4+ working groups – many white papers

- ATIS-I-0000034, PSTN Transition Focus Group Assessment section related to caller ID
- PSTN transition working group related to Caller ID



IETF has several initiatives

- STIR (Secure Telephony Identify Problem) which proposes passing encrypted cert between SIP / PSTN to authenticate caller ID
- Caller Preferences for the Session Initiation Protocol (SIP) to add extensions for handling
- Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

Details on Initiatives

Org	Overview	Initiative Name	Initiative Descriptions	Other Important Links
in2EPS	IETF and 3GPP consolidated information to ease the knowledge of the 3GPP Evolved Packet System	Study on security on spoofed call detection and prevention (Stage 2)	<p>This study item studies the detection of a spoofed call as the first step, and prevention as a second step if detection is achievable. In particular, the goals of this document are:</p> <ul style="list-style-type: none"> – Outline valid threat scenarios for spoofed calls coming to 2G and 3G CS domains; – Analyze and evaluate if any tools in 3GPP can be used to counteract spoofed call detection and prevention; – Study and identify any other suitable techniques or mechanisms for spoofed call detection and prevention. 	
M3AAWG	The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is driven by market needs and the insight of its global membership. With member companies from Asia, Europe, North America and South America, the organization currently is working on a variety of initiatives addressing ongoing and emerging messaging abuse issues, including bot mitigation, cooperative industry outreach, Web messaging abuse, DNS abuse, wireless messaging, senders issues and other topics.	Voice and Telephony Anti-Abuse Workshop	Open to the industry, government and academia, the upcoming Voice and Telephony Anti-Abuse Workshop will feature leading industry and government speakers addressing robocalls, caller-ID spoofing, voice phishing and other issues. Hosted by the M3AAWG VTA SIG, it will continue the work to identify key threats and actions to help reduce telephone services exploitation.	Published Documents

Appendix C

Org	Overview	Initiative Name	Initiative Descriptions	Other Important Links
3GPP	<p>The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.</p> <p>The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.</p>	Study on security on spoofed call detection and prevention (Stage 2)	SA WG3 is responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols. The WG also ensures the availability of cryptographic algorithms which need to be part of the specifications	3GPP Specification Details
				Download Specs from working group
3GPP	<p>The 3rd Generation Partnership Project (3GPP) unites [Six] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), known as “Organizational Partners” and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.</p> <p>The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, and quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.</p>	Security Working Group	SA WG3 is responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols. The WG also ensures the availability of cryptographic algorithms which need to be part of the specifications.	Specification FS_SPOOF

Appendix C

Org	Overview	Initiative Name	Initiative Descriptions	Other Important Links
ITU-T	The Study Groups of ITU's Telecommunication Standardization Sector (ITU-T) assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of information and communication technologies (ICTs). Standards are critical to the interoperability of ICTs and whether we exchange voice, video or data messages, standards enable global communications by ensuring that countries' ICT networks and devices are speaking the same language.	Workshop on "Caller ID Spoofing"	The main objective of this workshop is to present the current status of this issue in both of the PSTN and IP environments, and the relevant activities within and outside ITU-T, and to share experiences, analyze and discuss the issue from both technical and regulatory aspects, and to consider proposals on future activities and the potential of cooperation, based on a comprehensive understanding of this issue that could be achieved through this workshop.	http://www.itu.int/en/ITU-T/Workshops-and-Seminars/callerid/Pages/default.aspx
				Approved IETF Recommendation on Certificates
				International Calling Party Number Delivery, Calling Line Identification
GSMA	GSMA is an industry alliance organization.	Member White Papers on Caller ID	Go to http://www.gsma.com and type in "Secure Caller ID." Several papers and documents can be downloaded on industry and alliance organization members' thoughts on Caller ID security. Some examples are on the right.	Finnish Mobile ID
				Conference Calling and Caller ID
				Ecosystem to secure contact with end-users and collect information (video calls, telephone calls, caller ID, etc.)

Appendix C

Org	Overview	Initiative Name	Initiative Descriptions	Other Important Links
ATIS	ATIS - NGIIF	Next Generation Interconnection Interoperability Forum (NGIIF)'s mission is to address 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.	NGIIF Issue #031, Develop New Text Related to Methodologies That Support TDM/IP Caller ID Services, Call Spoofing, Etc.	<p>As a result of recently issued FCC reports and orders, the NGIIF has determined a business need to develop new text related to methodologies that support TDM/IP Caller ID Services, call spoofing, etc.</p> <p>A listing of 7 contributions to the ongoing effort is listed below.</p>
				Presentation by Henning Schulzrinne, Transitioning the PSTN to IP
				Henning Schulzrinne prstn to 2013-sipnoc.pptx
			Presentation by Henning Schulzrinne, Preventing Caller ID Spoofing	2013-nanc-spoofing.pptx
			Article on "International enforcement agencies join forces to thwart caller identification spoofing"	http://www.crtc.gc.ca/eng/com100/2013/r131021.htm#.UpZKqfso7IX
			ATIS-I-0000034, PSTN Transition Focus Group Assessment section related to caller ID	ATIS-I-0000034.pdf

Appendix C

ATIS			<p>DA 11-1089, Caller Identification Information in Successor or Replacement Technologies to determine if text needs to be augmented in ATIS-0300032, NGIIF Reference Document Part X- Interconnection Between LECs- Operations Handbook Local Interconnection Service Arrangement - Version 12.0 Section 7</p>	<p>DA 11-1089A1.pdf</p>
			<p>FCC 11-100, Rules and Regulations Implementing the Truth in Caller ID Act of 2009, to determine if text needs to be augmented in ATIS-0300032</p>	<p>FCC-11-100A1.pdf</p>
			<p>ATIS-0300032, NGIIF Reference Document Part X- Interconnection Between LECs- Operations Handbook Local Interconnection Service Arrangement - Version 12.0 Section 7</p>	<p>atis0300032.doc</p>

Appendix C

Org	Overview	Initiative Name	Initiative Descriptions	Other Important Links
IETF	<p>The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.</p> <p>Protocol ownership - when the IETF takes ownership of a protocol or function, it accepts the responsibility for all aspects of the protocol, even though some aspects may rarely or never be seen on the Internet. Conversely, when the IETF is not responsible for a protocol or function, it does not attempt to exert control over it, even though it may at times touch or affect the Internet.</p>	Secure Telephony Identify Problem Statement and Requirements (STIR)	Over the past decade, Voice over IP (VoIP) systems based on SIP have replaced many traditional telephony deployments. Interworking VoIP systems with the traditional telephone network has reduced the overall level of calling party number and Caller ID assurances by granting attackers new and inexpensive tools to impersonate or obscure calling party numbers when orchestrating bulk commercial calling schemes, hacking voicemail boxes, or even circumventing multi-factor authentication systems trusted by banks. Despite previous attempts to provide a secure assurance of the origin of SIP communications, we still lack effective standards for identifying the calling party in a VoIP session. This document examines the reasons why providing identity for telephone numbers on the Internet has proven so difficult and shows how changes in the last decade may provide us with new strategies for attaching a secure identity to SIP sessions. It also gives high-level requirements for a solution in this space.	RFC7340
			Secure Telephony Identify Revisited	STIR Charter
				Draft IETF Problem Statement
				Draft IETF STIR Threats
			SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks	Draft IETF SIP Privacy

Appendix C

Org	Overview	Initiative Name	Initiative Descriptions	Other Important Links
IETF		Caller Preferences for the Session Initiation Protocol (SIP)	This document describes a set of extensions to the Session Initiation Protocol (SIP) which allow a caller to express preferences about request handling in servers. These preferences include the ability to select which Uniform Resource Identifiers (URI) a request gets routed to, and to specify certain request handling directives in proxies and redirect servers. It does so by defining three new request header fields, Accept-Contact, Reject-Contact, and Request-Disposition, which specify the caller's preferences.	RFC 3841
		Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	This document describes private extensions to the Session Initiation Protocol (SIP) that enable a network of trusted SIP servers to assert the identity of authenticated users, and the application of existing privacy mechanisms to the identity problem. The use of these extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information. This document does NOT offer a general privacy or identity model suitable for use between different trust domains, or use in the Internet at large.	RFC3325

Appendix D

This appendix contains a list of acronyms

Acronym	Definition
2G	Second Generation of cellular telephone technology.
3G	Third Generation of cellular telephone technology.
3GPP	3rd Generation Partnership Project
ACR	Automatic Call Rejection - feature offered on AT&T voice services
ARIB	Association of Radio Industries and Businesses - standardization organization in Japan
ATIS	Alliance for Telecommunications Industry Solutions
ATIS-NGIIF	ATIS working group named Next Generation Interconnection Interoperability Forum
AVPN	AT&T Virtual Private Network - one of the MPLS offerings at AT&T
CCSA	China Communications Standards Association
DND	Do Not Disturb feature
DNS	Domain Named Service
ETSI	European Telecommunications Standards Institute
EVPN	Enhanced Virtual Private Network - one of the MPLS offerings at AT&T
GSM	Global System for Mobile Communications
GSMA	GSM Association
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
in2EPS	Organization name for into the 3G Evolved Packet System
IP	Internet Protocol
IPFlex	IP Flexible Reach - a SIP offering from AT&T
ITU	International Telecommunication Union
ITU-T	Abbreviation for the ITU's Telecommunications Standardization Sector
LEC	Local Exchange Carrier
M3AAWG	Messaging Malware Mobile Anti-Abuse Working Group
M3AAWG VTA SIG	M3AAWG Voice and Telephony Anti-Abuse Special Interest Group
MIS	Managed Internet Service - managed Internet service provided by AT&T
MPLS	Multi-protocol Label Switching
PBX	Private Branch Exchange
PSTN	Publicly Switched Telephone Network
RFC	IETF Request For Comment
SA WG3	3GPP group called Service and System Aspect Working Group 3 responsible
SE	Southeast
SIP	Session Internet Protocol
STIR	IETF working group called Secure Telephone Identity Revisited
TDM	Time Division Multiplexing
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association - standards organization in Korea
TTC	Telecommunications Technology Committee based in Japan
URI	Universal Resource Identifier
VoIP	Voice over Internet Protocol