AT&T Consultant/Vendor Sales Group
UPDATE
Winter 2007

inside...

kari's corner

It's been a busy fall, and the year is quickly coming to a close! But no matter the season, we continue to share leading-edge solutions to meet your clients' needs. Our vision is to connect people with their world, everywhere they live and work and do it better than anyone else. We hope that this newsletter is a strong connecting point with all of you!

In this edition, we're very happy to welcome back some old friends. Dave Deleese is back with us, writing about MPLS, and Paul Bedell contributes an in-depth overview of Mobile Advertising. You'll also learn about our convenient eBill service on the BusinessDirect Portal. Tom David, Nancy Grover and Jerry Hinek are back again, with their usual interesting and insightful articles.

The demand for what we do — connectivity — is accelerating. Our unique set of assets — wireless, wired, IP data, broadband, and our IP global network — put us in a great position to serve the mobility and bandwidth needs of our mutual customers. And the velocity will only increase.

From all of us at CVSG, thank you for your hard work and passion to serve our customers. We wish you a joyous Holiday Season, and all the best in 2008.

Kari Aguinaldo
CVSG Leader
415-644-7118
kw6875@att.com

in this issue...

UPDATE Editor
Elaine Tipping
elaine.tipping@att.com

Contributors
Kari Aguinaldo
Paul Bedell
John Cushman
Tom David
Dave Deleese
Nancy Grover
Jerry Hinek

Layout & Design
Lillian Cram
AT&T MultiMedia Productions

Publisher
AT&T West
Business Communications Services
Sales Operations

AT&T Customer Service Numbers

Pre-Merger SBC Areas:

California	Sales & Billing	Repair
Small Business	1-800-750-2355	611 or Toll-free 1-800-750-2355
Medium Business	1-800-891-1800	611 or Toll-free 1-800-332-1321

Nevada	Sales & Billing	Repair
Business/Consumer	1-800-288-2020	1-877-469-2355

Southwest	Business
Sales	1-800-499-7928
Billing	1-800-559-7928
Repair	1-800-286-8313

Midwest	Small Business Sales & Billing	Small Business Repair
Indiana	1-800-660-3000	1-800-727-2273
Wisconsin	1-800-660-3000	1-800-727-2273
Illinois	1-800-660-3000	1-800-727-2273
Ohio	1-800-660-3000	1-800-727-2273
Michigan	1-800-660-3000	1-800-727-2273
Español		1-800-426-2902

East (CT)	Sales & Billing	Repair
Business	1-800-448-1008	1-800-922-4646

Pre-Merger AT&T Mass Market Areas:

Local and Long Distance Service: 1-800-222-0300

AT&T CallVantage Service: 1-866-596-8464

AT&T Worldnet and DSL Service: 1-800-WORLDNET (1-800-967-5363)

AT&T Alascom (Alaska):

Business Services: 1-800-955-9556

MultiProtocol Label Switching (MPLS) – A Review

Greetings to the Consultant/Vendor community! It's been a few years (and a few lost hairs!) since my departure from the CVSG, and I certainly appreciate this opportunity to bring you some interesting information on products and services offered by the new AT&T.

After leaving the CVSG, I moved into the Out of Franchise group with Pacific Bell/SBC and was involved in the sales of data and voice services into the Independent Territories in California. I transitioned into the Specialized Markets group in 2006. I'm currently working with Alarm Companies, Answering/ Messaging Services, our Solution Providers and the AT&T Affiliates, providing for their data/voice needs.

The merger with AT&T brought us many new and powerful products and services that cover the full spectrum for voice, video and data services. The backbone network is evolving constantly, and specifically from TDM-based to IP Packet-based. Time Division Multiplexing (TDM) is very rigid and efficient but also very wasteful. Time slots can go empty and unused and the attitude of the network is, "Oh well". Traditional IP routing was a move in the right direction but needed to evolve to support the growing demands of the applications. The paradigm shift has been the move from "build a voice network and the data will ride for free" to "build a data network and the voice will ride for free". The infrastructure that allows for greater efficiencies for the convergence of voice, video and data is MultiProtocol Label Switching (MPLS).

The simple definition of MPLS is "an Internet Engineering Task Force (IETF)–specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network". As is the case for just about everything in telecom these days, it can all be "blamed" on the Internet. The Internet has inspired the development of quite a variety of applications for both the consumer and business markets. This forced a demand for increased and guaranteed bandwidth requirements in the backbone network. Initially, the network catered to simple applications like file transfer and remote login, but as the demand for higher speeds and the ability to support higher-bandwidth applications involving voice and multimedia emerged, more sophisticated switching hardware was required that allowed for the ability to manage the traffic at Layer 2 and Layer 3 more efficiently.

The initial goal of label-based switching was to bring the speed of Layer 2 switching to Layer 3. MPLS has been described as the Layer 2.5 protocol. Label-based switching methods allow routers to make forwarding decisions based on the contents of a simple label, rather than by performing a complex route lookup based on destination IP address. Other benefits to an IP-based network brought on by MPLS include:

- Traffic Engineering – the ability to set the path traffic will take through the network, and the ability to set performance characteristics for a class of traffic.
- VPNs – using MPLS, service providers can create IP tunnels throughout their network without the need for encryption or end-user applications.
- Layer 2 Transport – New standards being defined by the IETF allow service providers to carry Layer 2 services including Ethernet, Frame Relay and ATM over an IP/MPLS core.
- Elimination of Multiple Layers –

Continued on page 4

The paradigm shift has been the move from "build a voice network and the data will ride for free" to "build a data network and the voice will ride for free".

Continued from page 3

Typically most carrier networks employ an overlay model where SONET is deployed at Layer 1, ATM is used at Layer 2 and IP is used at Layer 3. Using MPLS, carriers can migrate many of the functions of SONET and ATM to Layer 3, thereby simplifying network management and minimizing network complexity. Eventually, carrier networks may be able to migrate away from SONET and ATM altogether, which means elimination of ATM's inherent "cell-tax" in carrying IP traffic.

In an MPLS network, incoming packets are assigned a "label" by a Label Edge Router (LER). Packets are forwarded along a Label Switch Path (LSP) where each Label Switch Router (LSR) makes forwarding decisions based solely on the contents of the label. At each hop, the LSR strips off the existing label and applies a new label which tells the next hop how to forward the packet.

Label Switch Paths are established by network operators for a variety of purposes, such as to guarantee a certain level of performance, to route around network congestion, or to create IP tunnels for network-based virtual private networks. In many ways, LSP's are no different than circuit-switched paths in ATM or Frame Relay networks, except that they are not dependent on a particular Layer 2 technology.

An LSP can be established that crosses multiple Layer 2 transports such as ATM, Frame Relay or Ethernet. Thus, one of the true promises of MPLS is the ability to create end-to-end circuits, with specific performance characteristics, across any type of transport medium.

One of the true promises of MPLS is the ability to create end-to-end circuits, with specific performance characteristics, across any type of transport medium.

The efficiencies realized in a Label Switched network allow for voice and video to transit easily and effectively as Quality of Service (QoS) and Class of Service (CoS) options are introduced to guarantee delivery of time-sensitive applications like voice and video. The labeling scheme along with the layer management introduces the capabilities to alleviate the pitfalls previously encountered in the old traditional networking methods. Additionally, private VPN's can be realized via tunneling through the core network with a variety of access links from DSL, Frame, ATM on up to Optical Ethernet connectivity.

Scalability and flexibility are truly the key buzz words with the advent of a MPLS core network. Many of the Legacy AT&T services we can now offer utilize the core MPLS network. VoIP services, PNT, which is essentially a private data network offering, and our NVPN offerings are IP-driven and are managed over the AT&T MPLS network. The growth in these types of services requires the depth in capabilities that MPLS allows for in the network. As the applications continue to develop in complexity and creativity, this core network will continue to evolve to accommodate them.

Dave DeLeese
Technical Consultant II
dd8121@att.com

john cushman

AT&T BusinessDirect® — eBill

One of the tools on the AT&T BusinessDirect® portal that customers rave about is — eBill. This tool enables customers to pay their AT&T bills online — in many cases through automatic electronic transactions — and it does much more.

One of the most valued benefits AT&T eBill delivers is that it makes it easier for customers to manage their telecom expenses by readily identifying trends. With just a few mouse clicks, customers can view standard reports, such as a month-over-month variance report, or custom reports that reflect their own way of doing business. Custom reports can be saved as templates for easy reuse each month.

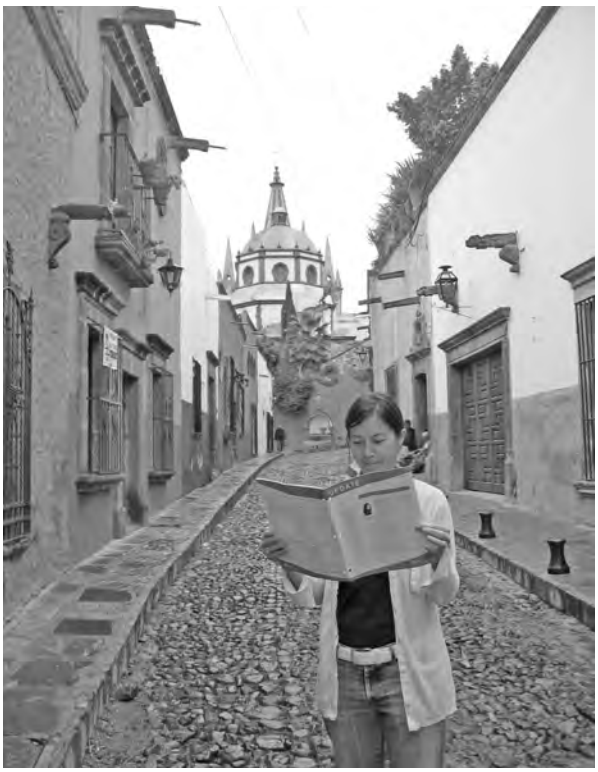
With AT&T eBill, customers receive their billing information sooner than it can be delivered by mail. And since the information is downloadable, they can store it conveniently and reduce their storage requirements for paper copies. This is a considerable benefit for large companies with voluminous bills.

Customers can also use AT&T eBill to dispute charges and track issue resolution online. Using this process, the charges in question are deducted from the bill while we research the inquiry.

AT&T eBill meets customer needs by offering efficient, effective telecom management capabilities online via the AT&T BusinessDirect portal. I look forward to sharing information on other BusinessDirect tools in upcoming *Updates*.

John Cushman
Vice President
AT&T eSales & Service

READ THE WORLD OVER



Voraciously reading the CVSG UPDATE in San Miguel de Allende, Mexico

nancy grover

Telling Computers and Humans Apart

If you've ever signed up for a free email account or bought tickets online, you've probably seen them; distorted characters that look like an eye chart from a carnival funhouse.

They're called CAPTCHAs, and they're used to verify that a human, not a computer, is submitting a request for a Web service. CAPTCHAs were originally created to protect Web sites from spammers and their bots. But lately, some have proved to be less than effective, as Ticketmaster recently learned. More on that later.

CAPTCHAs were originally created to protect websites from spammers and their bots.

CAPTCHA 101

The term CAPTCHA was coined in 2000 by a group of Carnegie Mellon University computer scientists to help Yahoo! combat spam. The acronym stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart.

"Turing" refers to Alan Turing, a British mathematician famous for designing an electromechanical machine that helped break Germany's encryption machine, The Enigma, during World War II. Later, in 1950, he developed the Turing test, a proposal to show a computer's ability to demonstrate intelligence.

In the test, a human judge was placed in one room, and another human and computer in another. Using text only, the judge would engage each in conversation. If the judge could not tell which was which, the computer would be said to have intelligence.

The CAPTCHA uses that same concept to distinguish between human and computer. And it does this by sending a random, distorted image to a user's browser that a real person can read, but theoretically, a machine can't.

For instance, when you sign up for a Yahoo! e-mail account, the site displays a group of warped numbers. Registrants are asked to type those characters into a box as part of the registration process. A human can read the characters, and ideally a computer can't. This keeps spammers from creating hordes of email accounts from which they can send spam.

CAPTCHAs in Action

In addition to creating free email accounts, spammers and fraudsters regularly use bots to identify Web pages that accept user data, and then send huge amounts of data to them, such as flooding discussion forums with unsolicited advertisements, or posting unwanted comments on blogs and social networking sites like Facebook and MySpace. Even online polls can fall victim to attacks where bots are used to effectively "stuff the ballot box." Unfortunately, the traffic generated by these bots can flood databases and degrade network throughput, making Web sites inaccessible.

That's where CAPTCHA verification comes in. It protects systems by ensuring data sent is from a person and not a bot. And it does this by asking the user to complete a test. While a computer generates and grades the test, it cannot solve the test. And because computers can't decipher a CAPTCHA, correct answers are assumed to be from a human.

Breaking CAPTCHAs

Some spam companies are getting around the challenge of CAPTCHAs by hiring workers to fill out forms for them instead of relying exclusively on bots. In one scheme, a bot fills out an online form and if it reaches a CAPTCHA, it's handed off to a human to solve and complete.

Others are rolling out new and improved bots that use Optical Character Recognition (OCR) to identify hidden words. It works by extracting the CAPTCHA image from a Web page, and removing any background colors or patterns. The image is then split into segments, each with a single letter or number. The bot then proceeds to identify each of those characters and retype them automatically.

Some computer scientists and hobbyists have solved CAPTCHAs to a 90% degree of accuracy using the same method. And that same technique may have been used by a company called RMG to bypass the Ticketmaster user verification system.

Ticketmaster posts CAPTCHAs on its site to prevent scalpers from buying enormous numbers of tickets to sell at a profit. However, software written by RMG and sold to ticket scalpers was able to automatically request tickets and solve the CAPTCHA in a matter of seconds. That resulted in popular concerts selling out within hours, with angry customers turning to those same scalpers for a ticket at many times the original cost.

A new CAPTCHA scam comes in the form of a Trojan, disguising itself as a game that lets players see images of a model undressing. In order to get the model to lose a piece of clothing, the user must solve a CAPTCHA. After several tries, the user soon realizes that the woman never fully removes her clothes, and gives up. But computer security experts think by then, the scammers got what they wanted – solved CAPTCHAs that can be used to try to break into legitimate sites.

It's these types of CAPTCHA hacks that are prompting computer scientists and Internet companies to find new CAPTCHA variations that keep it easy for humans to decipher, but harder for computers to crack.

Making CAPTCHAs Stronger

In an effort to stop new, smarter bots, CAPTCHAs are getting longer, and the characters more warped and twisted, and that's making it difficult for legitimate users to interpret.

To help, some Web sites have started rolling out new types of CAPTCHAs that involve solving simple random equations or answering easy questions, like, "what is 2+5?, or "what color is the sky?" Others are exploring the possibility of using image based CAPTCHAs where a user would be presented with a picture and asked to correctly identify it.

Then there's the problem of accessibility. The World Wide Web Consortium, the group that helps develop specifications for Internet technologies, is encouraging the creation of audio CAPTCHAs, so people with disabilities ranging from blindness to dyslexia and short-term memory problems can access protected Web services. A growing number of sites including Hotmail, PayPal and Google now offer audio CAPTCHAs as an alternative to their text-based verification system.

Even the original CAPTCHA development team from Carnegie Mellon is building their own audio-based CAPTCHAs, and they're recruiting volunteers to read text-based CAPTCHAs to help build up their audio database. And they're looking for volunteers to help with another project near and dear to their hearts – The reCAPTCHA.

Preserving Books, One CAPTCHA at a Time

reCAPTCHA is an ingenious system that puts the time a person uses to interpret a CAPTCHA to good use. 60 million CAPTCHAs are solved every day, each taking about 10 seconds to solve, which all translates to over 150,000 human hours each day spent deciphering CAPTCHAs. The reCAPTCHA system is harnessing all that time and energy to help digitize books for the Internet Archives.

The books and manuscripts were written before the Internet age, and number more than 100 million. To accomplish this daunting task, each page from each book is photographically scanned, and then transformed into text using OCR. But, OCR can't identify every word due to the poor quality of the original works.

reCAPTCHA solves that problem by sending words the computer can't read to a Web site in the form of a CAPTCHA and lets a human solve the puzzle. It does that by using two words: one that is already known by the computer and one the computer can't make out. If a user can solve the known word successfully, the system assumes it has solved the second word correctly as well. And just to make sure, the same two words are given to a number of other people. As more humans get the same answer, the more confident the system is that the unknown word is correctly identified.

Thanks to popular sites like Facebook, Twitter and StumbleUpon who are using reCAPTCHAs, the archiving project is deciphering one million new words every day. At this rate, what would have taken 400 years to accomplish can be completed in just a matter of decades.

Nancy Grover
Regional Manager
AT&T Corporate Information Security

In an effort to stop new, smarter bots, CAPTCHAs are getting longer, and the characters more warped and twisted, and that's making it difficult for legitimate users to interpret.

Small and medium size business customers are increasingly turning to Metropolitan Area Networks to provide transparent connections at continually higher speeds. Ethernet has played an increasingly significant role in this transport as customers have begun to migrate from circuit switched to packet switched services. Customers have found as the power of applications, PCs and work stations has increased, so too has their need to connect them at higher speeds.

Several years ago AT&T introduced OPT-E-MAN[sm] as an advanced, packet and fiber-based transport providing Layer 2 Ethernet service. OPT-E-MAN acts as an Ethernet bridge to transparently connect multiple customer local area networks within the same LATA. It is also used as an underlying dedicated Internet access transport. The product supports nearly any data transport configuration—point to point, point to multi-point, or multi-point to multi-point—using physical and virtual connections to meet specific business needs.

Until recently, OPT-E-MAN was out of reach for some small to medium size customer sites because fiber to transport service was out of their geographic and financial reach. OPT-E-MAN has been offered at 5 Mbps, 10 Mbps, 20 Mbps and above utilizing fiber. Beginning in early 2008 AT&T will offer OPT-E-MAN at 2 Mbps, 4 Mbps and 8 Mbps speeds to small business customers in selected offices. These are customers who have traditionally leased multiple T1 lines. AT&T will provision over fiber or, depending upon loop length, embedded copper reaching out to more customers.

The idea behind the slower "midband" speeds and the use of copper is to reach a larger swath of potential customers — smaller businesses just outgrowing T1s, and those that are not on our fiber network.

Many customers today utilize transport and packet-based services as a means for interconnecting two or more locations. This interconnection, done via bridges and routers, can be quite expensive and does not provide a lot of flexibility. OPT-E-MAN provides the means for customers to migrate their current LAN topologies to a new, faster standard. The AT&T Ethernet solution is a low cost, simple and flexible solution for small, medium and large businesses. It offers reliable and secure network architecture with an MPLS core, integrates seamlessly with pre-existing infrastructures, scales to LAN speeds, supports all topologies, and supports the most common enterprise applications.

Until recently, OPT-E-MAN was out of reach for some small to medium size customer sites because fiber to transport service was out of their geographic and financial reach.

Tom David
Liaison Manager
td1898@att.com

AT&T Launches AT&T Connect

AT&T has acquired Interwise, a leading global provider of Internet Protocol (IP)-based voice, Web and video conferencing services. In parallel, AT&T announced the launch of AT&T Connect, the first in a planned series of converged voice, video and web conferencing products and services for the delivery of unified communications to companies worldwide.

AT&T is rapidly integrating its wired and wireless network assets, over which it intends to deliver a portfolio of services to help businesses integrate all of their communications applications — wired and wireless voice services, conferencing capabilities, including VoIP, Web and video, and presence-based applications, such as instant messaging and directories.

AT&T's first unified communications solution is AT&T Connect, a converged IP conferencing service that provides unlimited voice, Web and video conferencing capabilities and can be scaled for businesses of all sizes. In addition to offering on-premises and fully hosted conferencing capabilities, AT&T will now be able to offer a unique, hybrid solution that allows enterprises to receive the cost and security benefits of on-site software with the rapid startup, geographic reach and capacity protection of its hosted service.

Energy and persistence conquer all things. — Ben Franklin

AT&T Regional Contact Information

REGION	States	Toll-Free Number	Fax Number	E-Mail Address
East	CT	800-448-1008		
West	CA, NV	800-733-3318	877-778-4133	vcsc@att.com
Midwest	IL, IN, OH, MI, WI	800-660-3000	312-456-8660	
Southeast	AL, FL, GA, KY LA, MS, NC, SC	877-866-8066		ind.vsc@bellsouth.com
Southwest	AR, KS, MO, OK, TX	800-241-0578	800-291-7123	swbtcog@att.com
Global/Enterprise	All	866-218-3976		sogisbus@txmail.sbc.com

Customer Service Record (CSR) requests may be faxed with a Letter of Agency (LOA) and a list of BTNs being requested with your contact information.

For simple and complex orders call toll-free numbers or e-mail your order information.

For questions or need help, please contact your Liaison Manager – 800-552-5299.

paul bedell

Mobile Advertising 101

Mobile advertising – hype or reality?

Reality. Soon.

That's right. Advertising will be coming to a mobile phone near you – specifically, your own mobile phone – in the near future. The mobile sphere represents the last bastion of the electronic communication world that hasn't been fully exposed to advertising yet. But that's about to change.

The mobile sphere represents the last bastion of the electronic communication world that hasn't been fully exposed to advertising yet. But that's about to change.

This is certainly one of the hottest discussion topics in the wireless industry. Although still a nascent business concept, mobile advertising is about to take off. Some wireless carriers have conducted trials to gauge effectiveness of mobile advertising. Other wireless carriers are simply making the leap by bravely launching mobile advertising.

Mobile advertising is a new kind of advertising channel that enables a much more effective business-to-customer communication. Advertisers and marketing experts recognize the unlimited opportunities presented by the mobile audience. The mobile market covers a huge potential customer base – people of all ages, sex, ethnic backgrounds, and socio-economic status have cell phone service. The target audience is now reachable all the time and anywhere. The mobile phone is the most personal communication device in history, and advertisers – like those who will communicate with us via wireless – have a unique opportunity to individually reach their target audiences as never before.

MOBILE AD TYPES

In the wireless world, the types of ads sent to mobile phones will largely mirror those used in the Internet world. There are certainly ad types that are unique to the mobile world as well.

Banner Ads, currently the most prevalent form of online ad, take the form of a graphic image that typically runs across the top of a Web page or is positioned in a margin or other space reserved for ads. When a banner ad appears on the left or right side of a Web page in an elongated vertical manner, it is known as a "skyscraper".

Banner ads may exist in a variety of formats including GIF, JPEG, Flash, HTML, Java, JavaScript and more, by typically conforming to a size standard. But most ads are animated GIF files, since animation has been shown to attract a larger percentage of user clicks. This "click through rate" (CTR) is a common metric used in the Web/mobile advertising world.

In addition to adhering to size, many Web sites limit the size of the ad file to a certain number of bytes so that the file will display quickly. Banner ads can appear on any type of Web page, in a Web application such as e-mail, or in an e-mail message. These ads are the most traditional type of Internet advertising, and give advertisers a presence in high traffic areas on the Web, which may typically be targeted based on a user profile or relevance to a user's past Web behavior. In summary, banner ads serve to reinforce the advertiser's brand.

Interstitial Ads are ads that appear between two content pages. They are also known as "transition ads", intermercial ads, a splash page or a flash page. An interstitial ad initiates play in a separate ad window during the transition between content pages. The ad continues while content is simultaneously being rendered. Depending primarily on line-speed, play of a transitional ad may finish before or after content rendering is completed. Advertisers who use interstitials generally have a captive audience who is waiting for their content to load. It can be intrusive, and the reaction of viewers depends on the relevance or

entertainment value of the message. An interstitial is usually designed to move automatically to the page the user requested, after allowing enough time for the message to register or the ad(s) to be read. What some consumers view as the best part of interstitial ads is the option, usually in the upper right hand corner, to "Skip This Advertisement". The potential annoyance factor is high with this type of ad.

Sponsorship Ads are ads that represent an association with a Web site or e-mail in some way that gives an advertiser a link to the content of the Web site. When associated with specific content, sponsorship can provide a more targeted audience than other types of ad buys. An affiliation with high-profile or well-known and respected content through a sponsorship can add to an advertiser's credibility. Through a sponsorship, an advertiser has the potential to reach a highly targeted market segment.

Key Word Ads are used when a key word search is undertaken. The key word can be purchased by advertisers in order to:

- Direct the hyperlink opportunity to the advertiser's site,
- To serve an ad related to the user's search, or
- To make their listing appear first.

Key word searches can be conducted through a search engine on a Web site. Key word search advertising can be effective because the user has already shown an interest in the product/service by performing the search, so they are reaching a captive audience.

Click-To-Call is a type of banner ad known as a "call-to-action" ad, specific to the mobile world. A banner ad has a hyperlink embedded with verbiage such as "call now" and is delivered to a wireless subscriber. Should the end user click to call, they'll likely be directed to the advertiser's call center, where they can obtain information on products or services, or request that information be sent to them. An order can also be placed for products or services.

Click-To-Buy Ads are also specific to the mobile world, and are essentially a subset form of click-to-call ads. The difference is that click-to-buy ads involve the opportunity to place an order for the products or services that are being advertised, and that's all. Unlike click-to-call ads, there's no option to "obtain information", etc. It's a commerce-based ad.

Coupon Ads are ads where a text coupon code can be delivered to a mobile customer, or displayed on the landing page of a Web site. Many times Common Short Codes (CSCs) are used in mobile advertising, where mobile subscribers are given a 5- or 6-digit string that serves as the address to issue a text message, whereupon the advertiser will respond to the subscriber with a coupon code or information on a sale at given merchant locations.

Offer-Based Ads are "clickable" ads that typically have some type of offer for end users.

Location-Based Ads are ads sent to mobile handsets, usually via text message or "offer-based ads", which are distinct because they're targeted to end users based on their geographic location. There are two categories of location-based ads: reactive ads and proactive ads.

A reactive location-based ad would allow a mobile subscriber to determine the location of "nearby stores" by sending an inquiry to the network, most likely through some type of Web-based GUI interface or text message using a Common Short Code. A text message response would then be sent to the mobile subscriber based on their location, telling them where the company's stores are within a given radius of that mobile customer (e.g., one mile or less).

Proactive location-based mobile advertising hasn't gained much traction yet for multiple reasons. It involves a mobile subscriber receiving a text message – an "offer-based ad" – that directly relates to their exact location. For example, if a mobile subscriber were in a mall walking by The Gap, they'd receive a text message stating, "Today Only, 25% Off All Gap Merchandise." The potential downside of proactive location-based mobile advertising is the comfort factor: mobile subscribers might

Continued on page 12

A reactive location-based ad would allow a mobile subscriber to determine the location of "nearby stores" by sending an inquiry to the network...

Continued from page 11

get "creeped out" knowing the wireless network knows their location down to the foot or yard.

In both reactive and proactive location-based ads, the advertising information would be directed to the mobile handset through a combination of locator technology and a geo-mapping database used by the wireless carrier (i.e., Geographic Information System – GIS – technology).

Run-Of-Site (ROS) Ads are placed to rotate on all "nonfeatured" ad spaces on a Web site. Pricing for run-of-site ads is usually less than rates for specially-placed ads or sponsorships.

Advergaming, the newest concept in marketing, allows companies to promote their products and services in a fun and entertaining way through games that potential customers play online, at home, and now, on their cell phones – without mobile customers paying for the receipt of the download. These games can be played from a link on a website, or through an e-mail message. Advergames offer the advertiser an opportunity for an extended impression with their brand in an entertainment, not advertising, context. Advergaming promotes products and services throughout a game's progress. Typically, downloading a game to a cell phone runs $2 to $8. But if a company agrees to pay for most or all of the game endorsement messages and download cost, the audience potential for promotion of that company's product or service becomes gigantic. That means the customer base created for those same products or services can grow exponentially. That's huge revenue for a relatively small investment.

Advergaming, the newest concept in marketing, allows companies to promote their products and services in a fun and entertaining way through games that potential customers play online, at home, and now, on their cell phones...

Pre-Roll Video Ads are videos that are placed to run before streaming video content or an interactive game. A pre-roll ad can be up to 30 seconds in length. The fast-forward functionality is disabled through the ad play. With pre-roll ads, advertisers can reach viewers who are increasingly watching more streaming video on the Internet in a way that the user cannot avoid since fast-forward is not enabled. This is currently a high growth area for consumer usage as well as available ad space.

Mid-Roll Video Ads are video ads that are placed to run within streaming video content or an interactive game. A mid-roll ad can be up to 30 seconds in length. The fast-forward functionality is disabled through the ad play. With mid-roll ads, advertisers can reach viewers who are increasingly watching more streaming video on the internet in a way that the user cannot avoid since fast-forward is not enabled. This also is currently a high growth area for consumer usage as well as available ad space.

Post-Roll Video Ads are video ads that are placed to run at the conclusion of streaming video content or an interactive game. There is no limit to the length that a post-roll ad can be. The fast-forward functionality is disabled through the ad play. The other factors mentioned above with pre-roll and mid-roll ads also apply here.

Pop-Up Ads appear in a new window which opens in front of the current one, displaying an advertisement, Web page, or entire Web site. These ad types are usually blocked due to the high annoyance factor associated with them.

Search Advertising is a method of placing online advertisements on Web pages (especially search engines) based on specific characteristics of the viewer. These could include search words entered by the viewer, as well as geographic location or profile of the viewer.

MOBILE ADVERTISING METRICS

Similar to the television world, where Nielsen ratings "prove the value" of advertisements in certain time slots, assigned to run in line with given programming, advertisers in the mobile world will demand some form of proof that their advertising investments are paying off.

Metrics used to validate the real or potential payback of mobile advertising will largely mirror the metrics currently used in the Internet advertising world. The mobile advertising metrics approach is logically intertwined with the fact that many forms of mobile advertising will mirror the main forms of Internet-based advertising.

Traditional media measurement companies are getting on board as well, when it comes to mobile marketing and advertising. Nielsen, the company that measures consumer patterns across all media, launched a new wireless measurement service in July 2007 that will track wireless Internet, video and content consumption among the country's 240 million wireless subscribers, just as it tracks viewing patterns on TV. Nielsen will roll out the program, called "Nielsen Wireless", in phases with a service called Mobile Vector. Using information from its "People Meter" tracking, it will provide wireless carriers with detailed demographic information on their subscribers including examples of what kinds of media their customers consume apart from the mobile phone. Carriers can then use this information to determine how to target content to their customers, and to which kind of advertising campaigns customers would be most amenable. Nielsen will augment that data with its own polling program, which will specifically track what types of mobile data services subscribers are using.

THE MOBILE MARKETING ASSOCIATION (MMA)

The Mobile Marketing Association (MMA), based in Denver, was formed in 2003. The MMA was formed specifically "to stimulate the growth of mobile marketing and its associated technology" and includes among its members VISA, CBS, AT&T, and the Associated Press. The MMA is a global organization with representation in over twenty countries. MMA members include agencies, advertisers, hand held device manufacturers, carriers and operators, retailers, software providers and service providers, as well as any company focused on the potential of marketing via mobile devices.

The MMA provides mobile Web (WAP) banner ad guidelines, and has modified existing mobile Web banner advertising specifications to include sizes that allow for the most optimal banner ad to be served to the mobile device.

In addition, new technologies offer the ability to determine the device types and screen resolutions as advertisements are being delivered, thereby allowing the correct size of advertisement to be served to the proper device, which provides a better experience for both the mobile audience and the advertisers as well. In all instances, if the device size is not recognizable, the current default ad standard is applied – a banner ad that can fit on most all mobile devices.

The MMA also provides mobile ad guidelines in terms of prohibiting ads that are misleading or deceptive, ensuring ads are in good taste, and prohibiting ads related to illegal products, to name the most far-reaching guidelines. Special categories of ads must also comply with existing voluntary industry guidelines which includes – but is not limited to – alcohol, tobacco, sweepstakes/promotions, and ads targeting children.

IMPLEMENTATION OPTIONS

Since mobile advertising is fairly nascent to the marketing world, it's a fair question to ask how it could and will be implemented. What forms will it take?

It's important that communication platforms are used to give a business the possibility to give the target groups exactly the messages they desire, and not just "spam" them with advertising that doesn't interest them. Steadily improving mobile communication technology is already sophisticated enough to make the dream of mobile entertainment a reality. Mobile advertising and mobile entertainment can be used together to create an extremely effective customer-bonding system.

Some real-world examples of the types of mobile ad campaigns businesses can launch are:

- An automotive banner ad with a dealer locator option. For example, a mobile subscriber types a zip code into a box, and the nearest dealer location is displayed.
- A fast food restaurant ad with a click-for-coupon option
- Retail store ad with sale information

Continued on page 14

...New technologies offer the ability to determine the device types and screen resolutions as advertisements are being delivered...

Continued from page 13

- Teenagers could opt in (via e-mail) to receive text coupons for a local pizzeria chain.
- Airline ad with e-mail registration option. For example, register to be notified by text message when a certain fare reaches a given dollar threshold.
- Based on a profile developed via an opt-in e-mail, text messages could be appended with advertisements. The profile would only serve ads based on a mobile user's "stated interests".

More than 90% of all mobile phones in the U.S. today are text-capable, representing almost 200 million subscribers in total. Approximately 60% of U.S. mobile phones are Internet-capable. Even less are MMS capable (multi-media messaging). So pushing ads to the mobile via text messaging is, by default, the most efficient means of reaching a targeted mobile audience.

It's important that communication platforms are used to give a business the possibility to give the target groups exactly the messages they desire, and not just "spam" them with advertising that doesn't interest them.

TARGETING AND RELEVANCE

Most wireless carriers are being very cautious about the launch and use of mobile advertising, for fear of the "annoyance" factor. There's a legitimate concern that there may be a subscriber backlash if they're annoyed by ads that are pushed to their phones, especially for a service where monthly premiums are paid. The industry believes that there are several ways to ameliorate this issue.

First, ensuring that any ads that are "pushed" to mobile customers are targeted and relevant to the subscriber's interests will certainly ease any potential aggravation a subscriber may feel. Second, wireless carriers may subsidize part of the monthly recurring charges of the customer's service in order to placate them. The thinking is that the reduction in the monthly charges for service will, in effect, be subsidized and offset by the revenue obtained from advertising fees.

How this model works remains to be seen, but logically it appears to be a sensible business approach to mobile advertising. In May 2007, a Q Research survey found that 32% of 11–20 year olds in Britain said they'd be "happy" to receive advertising messages to their mobile phones, but a much larger percentage – 71% – agreed that they'd be willing to receive ads if they were targeted to the subscriber's particular interests. The percentage increases to 76% if the ads are "in exchange for discounts or special offers", and rise to a lofty 82% if the ads are "in exchange for credit". Like everything in this world, there's another perspective. A June 2007 Ingenio/Harris poll of over 4000 adults found that 74% claim they most likely would ignore or delete an ad they received on a cell phone. The good news is that 26% of those users are doing something else with these ads.

GROWTH POTENTIAL

Even with the attendant growth hurdles that come with any new technology or business model, mobile advertising is still poised to grow exponentially. According to the research firm eMarketer, in the United States, mobile advertising is expected to grow from $421 million in revenue in 2006, to a $4.7 billion industry by 2011. Globally, the mobile ad market is expected to increase to $11.3 billion by that same year.

Mobile television and video subscription revenues grew 198% year-over-year to $146 million in the first quarter of 2007, according to Telephia. Approximately 8.4 million wireless customers now subscribe to some form of mobile video, representing nearly 4% of all U.S. mobile subscribers. Nearly half of the mobile video subscribers polled said they were willing to view ads on their cell phones in exchange for "something of value", according to Telephia. Telephia's perspective, which makes sense, is that consumers are used to seeing commercials on their TV at home, which has created a learned behavior that is transferring to mobile TV and making advertising more acceptable.

The wireless industry is also doing its part to foster the development and acceptance of mobile advertising. In May 2007, the GSM Association (a predominant worldwide digital wireless standard) announced it wants to enhance revenue and user experiences by setting standards and codes of

conduct for mobile advertising. The GSM Association (GSMA) is putting its weight behind a program designed to encourage common standards and proper conduct for mobile advertising to ensure the medium is as successful as possible.

In addition to establishing standards, the GSMA – which represents more than 700 wireless carriers who collectively serve almost two-and-a-half billion users – aims to put metrics in place to measure the effectiveness of mobile ads. The GSMA also intends to ensure that any marketing techniques deployed add value to, rather than detract from, the mobile experience for users, by balancing the needs of communication and data collection with privacy concerns. According to Bill Gajda, chief commercial officer for the GSMA, "The mobile phone can offer advertisers a level of immediacy, intimacy and personalization that cannot be matched by other mediums. To realize this potential, the mobile industry, the advertising industry and the content industry need to come together to better define what advertising should look like on a mobile phone and how its effectiveness should be measured." The initiative, directed by the GSMA's Mobile Media and Entertainment Group, will press for change to optimize advertising on the so-called "fourth screen" by consulting with industry players and collectively taking action. It's likely the GSMA will at some point collaborate with the MMA in these endeavors.

"The opportunities of the mobile entertainment and advertising market are both vast and challenging," said Ben Hirsch, director of market development for group customer marketing at Orange (a European wireless carrier), one of the founding members of the GSMA's Media and Entertainment Group. "By working together to define a common approach to formats, delivery, inventory management and measurement, the carrier community can ensure that it serves both advertisers and customers in the most effective ways possible."

Although still in its infancy, the mobile advertising world appears to have an interesting and dynamic future.

Paul Bedell
AT&T Integrated Advertising and Commerce
pb1321@att.com

"...The mobile industry, the advertising industry and the content industry need to come together to better define what advertising should look like on a mobile phone and how its effectiveness should be measured."
–Bill Gajda
GSMA

FROM THE ARCHIVES

Photo Courtesy of SBC Archives and History Center, San Antonio, TX

Mobile telephone on car dashboard (1955)

jerry hinek

PCI Compliance

Introduction

You probably have relationships with businesses that take credit and debit cards from customers. These businesses must comply with Payment Card Industry (PCI) Data Security Standards (DSS). PCI audits and issues fines to businesses that are out of compliance. While PCI protects businesses, its primary aim is to protect payment card information from unauthorized access and use. You should go beyond the scope of PCI in protecting your own business and your clients.

...While PCI helps a firm to protect itself, its primary aim is to protect payment card information from unauthorized access and use.

Specifically, PCI DSS does not address any other information your business relies on, nor does it tell you how to protect that information. It does not say much about disaster recovery or business continuity in case of fire, flood, earthquake or other disaster. It does not mention appropriate insurance coverage for your business. If your business, or your client's business accepts payment cards, take this standard as a starting point.

Recent news articles indicate retailers are complaining to PCI that the standards place too much responsibility on them to retain and protect information that ought to be retained by banks alone. It's not so much a complaint with the standards but a conflict over who should be assigned the risks and responsibilities of keeping and protecting payment card information. This is an important issue that may have to be resolved in future DSS versions.

This article will discuss the PCI standards at a high level and give you direction for getting more information. It summarizes and paraphrases the DSS, and is not meant to be a substitute or replacement for the PCI DSS. To comply with PCI DSS you should study the actual document. The entire 16-page PCI DSS is available for free download on the Payment Card Industry home page: (https://www.pcisecuritystandards.org/). The standard requires a technical reading. The PCI DSS is not a tutorial telling you how to do these things. It is up to you either to have or to hire the expertise for compliance.

PCI Overview

The PCI DSS consists of 12 requirements divided among six control objectives. The 12 requirements are broken into more detailed sub-requirements. Table 1 is a reformatted version of the outline on page 1 of the PCI DSS.

Build and Maintain a Secure Network

The first control objective is concerned with building and bounding a secure network for processing, transmitting and storing cardholder data.

Requirement 1 discusses firewall configuration. It requires set up of a secure perimeter around your business network that protects cardholder data from inappropriate or illegal access from the Internet. The key points are:

- Establishment of firewall configuration standards.
- Permit only network traffic that is necessary for the environment and prohibit all other.
- Restrict connections between publicly accessible servers, such as web servers, and internal systems or servers that process cardholder data.
- Don't permit anyone from the Internet to gain unauthorized knowledge of the internal network.

Requirement 2 is concerned with proper configuration of the components of your business network. The key points are:

- Change vendor-supplied default

settings and values.

- Harden systems and address all known vulnerabilities.
- Encrypt administrative system communication over the network.

These are good requirements for any business that relies on a network. The bigger the business, the more complicated the network, and the more it has to protect itself. Both the network and the components of the network must be protected.

Protect Cardholder Data

While the whole PCI DSS mandates protection of cardholder data, this control objective discusses protection of the actual data, bits, bytes and paper representations of the data.

Requirement 3 protects cardholder data in storage, including display on paper. The key points are:

- Store only the cardholder that you really need for business or legal purposes and store it only as long as it's needed, then remove it securely from your systems.
- Don't store the authentication data once a user of the system is authenticated.
- Don't display the entire Primary Account Number (PAN) except to employees who need to see the entire number. Already on credit card receipts and emails, we only see the last four digits. Display only what is sufficient, and no more than the first six and last four digits.
- When storing the PAN, it must be unreadable. Normally this would be done with encryption or hashing.
- Protect the encryption keys used to conceal the PAN.
- Document how you manage your encryption keys.

Requirement 4 protects cardholder data in transit on the network. The two key points are:

- Use strong encryption.
- Never send the PAN in cleartext in email.

These requirements recognize that the PAN must be displayed and stored, but must always be protected.

Maintain a Vulnerability Management Program

This control objective contains information about protecting the computing systems and software on a network that contains payment card data.

Requirement 5 is about deployment of anti-virus software.

Continued on page 18

The bigger the business, the more complicated the network, and the more it has to protect itself.

Table 1

A. Build and Maintain a Secure Network
1) Install and maintain a firewall configuration to protect cardholder data
2) Do not use vendor-supplied defaults for system passwords and other security parameters

B. Protect Cardholder Data
3) Protect stored cardholder data
4) Encrypt transmission of cardholder data across open, public networks

C. Maintain a Vulnerability Management Program
5) Use and regularly update anti-virus software
6) Develop and maintain secure systems and applications

D. Implement Strong access Control Measures
7) Restrict access to cardholder data by business need-to-know
8) Assign a unique ID to each person with computer access
9) Restrict physical access to cardholder data

E. Regularly Monitor and Test Networks
10) Track and monitor all access to network resources and cardholder data
11) Regularly test security systems and processes

F. Maintain and Information Security Policy
12) Maintain a policy that addresses information security

Continued from page 17

- Use anti-virus software.
- Keep anti-virus software current with the latest signatures and software updates.

Requirement 6 is concerned with development and maintenance of secure systems and applications. Computer operating systems and application software tend to be very large and complex and they have vulnerabilities. Most of the vulnerabilities are only exposed by people working hard to break the code by trying to get it to do something it was not designed to do. Frequently this is accomplished by sending the program too much data or data specially crated to contain operating system instructions. PCI DSS requires these safeguards:

- When software vendors issue vulnerability patches, install them within a month.
- Make it a practice to be informed and aware of vulnerabilities as they are made known by security alerting services.
- If you develop software applications, follow industry best practices and build in security from the beginning.
- Have a secure process for updating software so that only approved updates are made to systems. You must also be prepared to back-out software updates that fail in production and to restore the previous versions if necessary.
- Pay special attention to Web applications. They reside on exposed servers and are more accessible to attackers.

There are many sources of vulnerability information, some by paid subscription and some free. Software and hardware vendors publicize available patches.

Implement Strong Access Control Measures

Access control measures are the means of restricting authorized people or systems to approved rights on systems, and prohibiting unauthorized people from any access.

Requirement 7 has two key points:

- Limit cardholder information access to those whose jobs require the access.
- Prohibit, by default, any access that is not explicitly permitted.

Requirement 8 mandates assigning unique identification to each person with authorized access to critical data and systems. In order to comply with requirement 8:

- Each system user must have a unique user name.
- Users must be authenticated with passwords, tokens or biometrics.
- Remote users are presented with two-factor authentication. Frequently the two factors would be a password and a token.
- Passwords must be encrypted both when transmitted and when stored.
- Follow a detailed set of standards to manage all authentication and passwords for non-consumer users on systems.

Requirement 9 addresses physical access to data. Physical access means both people who physically enter buildings or other facilities and who have access to hard-copy representations or media stores of cardholder data. The key points are:

- Have entry control at doors. This could be guards or doors that will open only when presented with a physical token or smart-card device.
- It must be easy to identify and distinguish visitors and employees.
- Visitors must follow procedures when entering and leaving.
- Visitors must be logged.
- Media backups should be stored securely and stored off-site if possible.
- Control the distribution and access of media.
- Destroy media that is no longer needed or required legally.

Even though cardholder data is used during business transactions by employees and customers, the burden is on the business to make sure that only authorized persons have access to this data.

Even though cardholder data is used during business transactions by employees and customers, the burden is on the business to make sure that only authorized persons have access to this data.

Regularly Monitor and Test Networks

This control objective goes along with the first control objective to build and maintain a secure network. Networks must be monitored and tested to keep them secure.

Requirement 10 specifies what to do when monitoring access to network and cardholder data.

- System components must automatically track user access and save an audit trail.
- Keep the audit trails secure from unauthorized access or modification.
- Review the audit trails daily for unusual or inappropriate activity.
- Retain the audit trails for a year.

Requirement 11 is about the discovery and correction of weaknesses through regular testing of security systems and processes.

- Look for internal and external vulnerabilities.
- Perform penetration testing annually or after making significant upgrades.
- Monitor file integrity; make sure the software and files haven't changed outside normal access and change controls.

Maintain an Information Security Policy

The policy is what informs your employees and contractors what your expectations are concerning maintaining a secure environment. Your policy should be tailored to your business, and should protect both cardholder data and the rest of your valuable business information.

Requirement 12 specifies the following standards:

- Establish and publish a policy for your employees that enforces the PCI DSS.
- Create operational procedures to comply with PCI DSS.
- State what is appropriate uses for system users and what is not appropriate.
- Identify responsibilities for employees and contractors.
- Have a security awareness program that informs employees and contractors of the need to protect cardholder data
- Contracts with business partners and service providers should enforce PCI DSS requirements for any cardholder data shared between partners.
- Have a plan to respond immediately to any system breaches.

Appendices

Appendix A identifies additional requirements and special considerations service providers, including host providers, must follow to protect the hosted environment and access to cardholder data.

Appendix B states some compensating controls when an entity is not capable of complete technical compliance with the DSS.

Conclusion

The PCI DSS is a very important document. People and business should be motivated on many levels to comply. For a business there is the risk of loss of consumer confidence or financial liability if payment card information is accessed by unauthorized persons. For each of us, as users of payment cards, there is the desire to protect our own good names and credit histories. There is some disagreement about where payment card information should be stored and who should assume the costs and risks for doing so. It's important to keep in mind that PCI DSS primarily protects cardholder information, not your business. You have to start with your own policy for your own business, and make sure that your own security needs are addressed as well as the requirements of PCI.

Jerry Hinek, CISSP
Senior Business Security Manager
AT&T Information Services

Your policy should be tailored to your business, and should protect both cardholder data and the rest of your valuable business information.

Helpful Numbers and Web Sites

Area Code Information
http://areacode-info.com/

Area Code Look Up
http://www.my-areacode.com/

AT&T BusinessDirect®
1-800-221-0000 Hot Line
http://www.att.com/businessdirect

AT&T Corporate Contact List
http://sbc.com/contactus

AT&T Customer Support
http://sbc.com/help

AT&T Local Service (repair desk)
1-800-829-1011

AT&T Product Information
http://ask.att.com

Billing Inquiry – West
1-800-891-1800

Carrier Verification
Pre-subscribed Interexchang Carrier (PIC) for long distance calling – 1-700-555-4141
Local Pre-subscribed Interexchange Carrier (LPIC) for intra-LATA, intrastate calling –
1-805-700-4141 – when calling in area codes 213 and 818
1-NPA-700-4141 – when calling in all other California area codes (substitute your area code for NPA)

CVSG Web Site
www.att.com/cvsg

DSL
1-877-722-3755

E-Bill
1-888-700-5422

FOCUS
http://www.thefocus.org

Internet Safety
http://att.com/safety

Knowledge Network
http://www.kn.att.com/products/discounts.html

Local Calling Area Mapping
http://localcalling.sbc.com/LCA/lca_input.jsp

Managed Internet Service
1-888-613-6330

North American Numbering Plan Administration
http://www.nanpa.com/

Priority Repair
1-800-332-1321

Up2Speed Newsletter
http://att.com/up2speed

AT&T Consultant/Vendor Sales Group

Kari Aguinaldo, CVSG Leader
795 Folsom St Rm 517-O2
San Francisco, CA 94107
415-644-7118
email: kw6875@att.com

Mike Aaron, Liaison Manager
795 Folsom St Rm 517-P3
San Francisco, CA 94107
415-644-7129
email: ma2519@att.com
Area codes: 209, 408, 415, 510, 559, 650, 707, 831, 916, 925
States: AL, AR, CO, FL, GA, HI, KS, KY, LA, MD, MS, MO, NM, NC, ND, OK, SC, TN, TX, VA, WV

Eric Aguirre, Data Administrator
email: ea3515@att.com

Consultant/Vendor Sales Group Hot Line
1-800-552-5299

Tom David, Liaison Manager
200 Center St Promenade Rm 735
Anaheim, CA 92805
949-855-5055
email: td1898@att.com
Area codes: 619, 714, 760, 858, 909, 949, 951
States: AK, AZ, CT, DE, ME, MA, NV, NH, NJ, NY, PA, RI, UT, VT

Lowayne Shieh, Liaison Manager
1150 South Olive St Rm 1600
Los Angeles, CA 90015
213-743-5759
email: ls1869@att.com
Area codes: 213, 310, 323, 424, 562, 626, 661, 805, 818
States: ID, IL, IN, IA, MI, MN, MT, NE, OH, OR, SD, WA, WI, WY
Country: Canada

Vendor Consultant Service Center (VCSC)
1-800-773-3318

LOA
Fax 1-877-778-4141 / 4133

AT&T West Alliance Channel (registration required)
https://west.alliance.att.com

at&t
Your world. Delivered.℠