EXHIBIT EE

Brett L. Gibbs, Esq. (SBN 251000)
38 Miller Avenue, #263
Mill Valley, CA 94941
415-325-5900
blgibbs@wefightpiracy.com

Withdrawing Attorney for Plaintiff

Paul Duffy (Bar No. 224159)
Anti-Piracy Law Group
161 N. Clark St., Suite 3200
Chicago, IL 60601
Phone: (800) 380-0840
E-mail: paduffy@antipiracylawgroup.com

Incoming Attorney for Plaintiff

IN THE UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF CALIFORNIA

AF HOLDINGS LLC,

Plaintiff,

v.

ANDREW MAGSUMBOL,

Defendant.

No. 3:12-cv-04221-SC

MOTION FOR WITHDRAWAL AND SUBSTITUTION OF COUNSEL

MOTION FOR WITHDRAWAL AND SUBSTITUTION OF COUNSEL

Brett L. Gibbs, counsel for Plaintiff AF Holdings LLC (“Plaintiff”), hereby moves the Court pursuant to Eastern District of California Local Rule (“L.R.”) 182(g), for an order permitting him to withdraw as counsel of record for Plaintiff in this action. Concurrently, attorney Paul Duffy hereby moves the Court for permission to be substituted in place of Brett L. Gibbs as attorney for Plaintiff.

As grounds for this Motion:

1. Brett L. Gibbs has been counsel for Plaintiff since the commencement of the action.

2. Brett L. Gibbs wishes to withdraw as counsel for Plaintiff.

3. Brett L. Gibbs has provided written notice of his withdrawal to Plaintiff. The client understands and accepts the withdrawal of Brett L. Gibbs.

4. Brett L. Gibbs has provided written notice of his withdrawal to all other parties who have appeared in this case, and there were no objections.

5. Paul Duffy is licensed to practice in the Eastern District of California, and requests that he be designated Counsel of Record on behalf of Plaintiff.

6. Brett L. Gibbs, Paul Duffy, and Plaintiff are all in agreement that this withdrawal and substitution are necessary to allow this case to proceed.

WHEREFORE, the Court should grant Brett L. Gibbs' and Paul Duffy's Motion for Withdrawal and Substitution of Counsel.

DATED: January 30, 2013.

Respectfully Submitted,

By: /s/ Brett L. Gibbs, Esq.

Brett L. Gibbs, Esq. (SBN 251000)
38 Miller Avenue, #263
Mill Valley, CA 94941
blgibbs@wefightpiracy.com
415-325-5900

Withdrawing Attorney for Plaintiff

Respectfully Submitted,

By: /s/ Paul Duffy

Paul Duffy (Bar No. 224159)
Anti-Piracy Law Group
161 N. Clark St., Suite 3200
Chicago, IL 60601
Phone: (800) 380-0840
E-mail: paduffy@antipiracylawgroup.com

Incoming Attorney for Plaintiff

By: /s/ Brett L. Gibbs, Esq.

Brett L. Gibbs, Esq.
In-House Counsel, AF Holdings LLC

IT IS SO ORDERED.

Dated: ______________________________ ______________________________________
United States District Judge

CERTIFICATE OF SERVICE

The undersigned hereby certify that on January 30, 2013, all individuals of record who are deemed to have consented to electronic service are being served a true and correct copy of the foregoing document, and all attachments and related documents, using the Court's ECF system.

/s/_Brett L. Gibbs_____	/s/ Paul Duffy
Brett L. Gibbs, Esq.	Paul Duffy

EXHIBIT FF

EXHIBIT FF

IN THE CIRC''IT COURT OF THE TWENTIETH JUDICIAL CIRCUIT
ST. CLAIR COUNTY, ILLINOIS
LAW DIVISION

GUAVA, LLC, Petitioner, v. COMCAST CABLE COMMUNICATIONS, LLC, Respondent.	)	Case No. 12-MR-417 Honorable Judge Andrew J. Gleeson

OPPOSITION TO MOTION TO QUASH

An attorney purporting to act on behalf of one "John Doe" ("Movant") identified only by **Internet Protocol ("IP") address 68.58.68.84** has filed a "Motion to Quash, Motion for Protective Order and Application to Proceed Under Fictitious Name." The Movant also filed a Motion for of an Order for Rule to Show Cause for various fictitious complaints about Plaintiff and its undersigned counsel, which even if true (they are utterly false) the nonparty Movant could not assert. (The two motions are referred to collectively as "Motion" or "Mot.")

The Motion is festooned with irresponsible, factually baseless and false statements on a number of subjects. The Movant has violated a number of Illinois Supreme Court rules, the Illinois Code of Civil Procedure and other governing laws. Among other things, the Movant --- not a party here --- has chosen to amend the caption so that rather than identifying the Plaintiff, it names a non-party, which has no corporate or other relation to the Plaintiff, as "Lightspeed Media Corporation d/b/a, a/k/a/ Guava, LLC." Nonparties, of course, are not permitted to unilaterally change case captions and substitute a party for a non-party when filing a discovery motion. Furthermore, the Movant has filed what it purports to be a "Rule 237 Notice to

Produce" for the hearing, in which it (again, a nonparty) seeks to compel appearances of "Alan Moay" [sic], counsel for Plaintiff, the owner of nonparty Lightspeed Media Corporation, "all officers, directors, managers and other Guava LLC and Lightspeed personnel responsible for" filing the Petition in this case. A nonparty has no right or standing to compel the appearance of parties or other nonparties at a motion hearing under Rule 237, and the filing is baseless and frivolous.

Movant's counsel has acted vexatiously and wantonly in filing its papers. Despite many requests to "quash" a "subpoena," there is no subpoena; the Court entered an Order on December 14, 2012 directing Comcast Cable Communications LLC to produce the Movant's identifying information. And Illinois Supreme Court Rules sharply limit the grounds upon which a nonmovant may object to discovery, which Movant, through its attempts to assert multiple conspiracy theories, has strayed far beyond. Even if it had the right to assert defenses and challenge the sufficiency of the Petition (which as a nonparty, the Petitioner does not), its arguments fail.

Petitioner has filed a combined omnibus response to the motions to quash filed in this action. To the extent the Movant here includes in its Motion the same arguments addressed in the omnibus response, Petitioner incorporates its responses by reference as if fully set forth herein. The remainder of Movant's argument is baseless, frivolous, false and impermissible for a nonparty to make. The Court should deny its Motion to "Quash" and its Motion for Entry of Rule to Show Cause. Moreover, the Court should strike its Rule 237 Notice to Produce.

LEGAL STANDARD

The Illinois Supreme Court's Rules "are not aspirational; rather, they have the force of law." *Bright v. Dicke*, 166 Ill.2d 204, 210, 652 N.E.2d 275, 277-78 (1995). They expressly limit the grounds upon which nonparties, such as Movant, may object to a subpoena. The Movant here has recklessly and vexatiously strayed beyond those limitations.

Illinois Supreme Court Rule 201 permits a party to "obtain by discovery full disclosure regarding any matter relevant to the subject matter involved in the pending action, whether it relates to the claim or defense . . . ." Ill. Sup. Ct. R. 201(b)(1). Illinois Supreme Court Rule 224 permits a party to identify unknown defendants so it can bring an action against them. *John Gaynor v. Burlington Northern and Santa Fe Railway*, 750 N.E.2d 307, 312 (Ill. App. Ct. 2001) ("Rule 224's use is appropriate in situations where a plaintiff has suffered injury but does not know the identity of one from whom recovery may be sought."); *Roth v. St. Elizabeth's Hospital*, 607 N.E.2d 1356, 1361 (Ill. App. Ct. 1993) ("[Rule 224] provides a tool by which a person or entity may, with leave of court, compel limited discovery before filing a lawsuit in an effort to determine the identity of one who may be liable in damages.") (Quoting 134 Ill. 2d R. 224, Committee Comments, at 188-89)). Once the identities are obtained a separate action is necessary to actually litigate the claims. *Roth*, 607 at 1360 ("Once the identity of such persons or entities has been ascertained, the purpose of the rule has been accomplished and the action should be dismissed.").

Illinois Supreme Court Rule 201, and the case law interpreting it, clearly establishes the grounds upon which a nonparty may object to a subpoena served upon it. The Movant here has not established that any of those grounds exist, and it does not have standing to make the substantive challenges to the Complaint, and assert defenses to liability, that are available only to the actual parties to a lawsuit.

I. IMPERMISSIBLE RULE 237 "NOTICE TO PRODUCE."

Movant accompanies its Motions with a purported notice pursuant to Illinois Supreme Court Rule 237(b) seeking to compel Plaintiff's officers, directors, managers and others to appear, along with nonparties Lightspeed Media Corporation, Steve Jones and Plaintiff's undersigned counsel. The purported notice fails for several reasons.

Rule 237(b) provides:

> **Rule 237. Compelling Appearances of Witnesses at Trial**
>
> **(b) Notice of Parties *et al.* at Trial or Other Evidentiary Hearings.** The appearance at the trial or other evidentiary hearing of a party or a person who at the time of trial or other evidentiary hearing is an officer, director, or employee of a party may be required by serving the party with a notice designating the person who is required to appear. The notice also may require the production at the trial or other evidentiary hearing of the originals of those documents or tangible things previously produced during discovery. If the party or person is a nonresident of the county, the court may order any terms and conditions in connection with his or her appearance at the trial or other evidentiary hearing that are just, including payment of his or her reasonable expenses. Upon a failure to comply with the notice, the court may enter any order that is just, including any sanction or remedy provided for in Rule 219(c) that may be appropriate.

Rule 237 by its own terms is limited to notice "of parties" to "a party or a person … [who] is an officer, director, or employee of a party…" Movant of course is not a party, and Rule 237 does not provide it any basis to compel anyone to appear at a trial or other evidentiary hearing. Its Rule 237 notice is not a "Notice of Party" and the Court should strike it. Furthermore, the purported notice seeks to compel the attendance of several non-parties: Alan Moay, undersigned counsel and Steve Jones. The notice is defective for that reason as well.

II. ARGUMENTS RELATING TO VERIFICATION ARE INVALID.

Movant also expends considerable time and vitriol taking issue with the verification on the Petition. Movant lacks standing to raise that issue, and in any event, its arguments and invectives relate to a name other than what appears on the Petition.

As set forth above, Movant lacks standing to raise sustentative challenges to the Petition because it is not a party. Such challenges fall far beyond what a nonparty may use to challenge a discovery request. Comcast, an actual party here, did not challenge the verification. The Petition upon its face shows that it was verified, and notarized; the Movants have based their claims on the pointless inquiry of whether a name other than that appearing on the Petition is valid.

Illinois Supreme Court Rule 224's only requirement relating to verification is that the petition must be "verified." R. 224(a)(1)(ii). The Petition is clearly verified. Movant seeks to challenge the verification on the ground that its attorney was unable to identify a person named "Alan Moay" through whatever research he performed or caused to be performed. He need not have bothered because that name does not appear on the Petition. Alan Mony, not "Moay," verified the Petition. Furthermore, that was notarized by a notary public. If Movant seeks to challenge the Petition (which as a nonparty he may not), he should focus on the actual person signing and the fact that it was notarized.

III. PETITIONER WILL USE MOVANT'S IDENTIFYING INFORMATION TO PROTECT ITS COMPUTER SYSTEMS.

Movant argues that Petitioner is seeking its identifying information solely to coerce Movants into settlements. (Mot. at 3-4.) Movant goes to great length to portray itself as a victim in this matter and is seemingly outraged that Petitioner would seek its identifying information. But in reality, Movant hacked into and tampered with Petitioner's protected computer systems. Movant put Petitioner's company and livelihood at risk by its actions. Petitioner simply wishes to identify the individual(s) that participated in these actions and hold them accountable. While Movant understandably does not want to be held accountable for its unlawful actions, its groundless and unsupported arguments are not a basis to prevent the release of the identifying information.

Petitioner has every intention of litigating its claims against those that hacked into its computer systems. That being said, public policy favors settlement. *Wal-Mart Stores, Inc. v. Visa U.S.A. Inc.*, 396 F.3d 96, 116-17 (2d Cir. 2005); *accord Williams v. First Nat'l Bank*, 216 U.S. 582, 595 (1910) ("Compromises of disputed claims are favored by the courts."); *TBK Partners, Ltd. v. W. Union Corp.*, 675 F.2d 456, 461 (2d Cir. 1982) (noting "the paramount policy of encouraging settlements"). For Plaintiff to reach a private resolution of its claims with those who hacked into it computer systems—in lieu of taking a matter to trial—is not abusive, but encouraged. The only choices available to Petitioner are to avail itself of the legal process or to accept the hacking of its systems. Proper use of the legal process cannot plausibly serve as a basis for the relief Movants seek.

Movant further argues that its identifying information should not be released because it will be embarrassed if its names are linked to the adult content associated with Petitioner. Movant essentially argues that because Petitioner's business is associated with adult content, Petitioner should not be allowed to protect its rights through the legal system. Petitioner is, not surprisingly, upset by the prospect of inferior access to the courts by virtue of its participation in the adult industry.

Petitioner has a constitutional right of access to the courts. Just because Petitioner may arguably be an unpopular litigant (e.g. an adult content producer) does not mean it should be denied access to the courts. Litigation is inherently embarrassing for everyone involved, including Petitioner, but that does not prevent them being able to seek justice through the courts.

IV. NO BASIS TO PROCEED ANONYMOUSLY.

Movant has failed to show (Mot. at 5) any valid basis to proceed anonymously. Illinois law strongly disfavors the use of fictitious names in judicial proceedings. At common law, suits involving fictitious parties were considered to be void *ab initio*. *Bogseth v. Emanuel,* 166 Ill.2d 507, 513, 655 N.E.2d 888 (1995). The reason is that courts only have subject matter jurisdiction over justiciable matters, which are matters in controversy between an actual plaintiff and an actual defendant. *Id.* at 514. The use of a fictitious name in Illinois must be explicitly authorized by statute in order for a court to have jurisdiction, and because they are in derogation of the common law, statutes authorizing the use of fictitious names must do so explicitly. *Id.* at 507; citing *Hailey v. Interstate Machinery Co.,* 121 Ill. App. 3d 237, 238, 459 N.E.2d 346 (3d Dist. 1984).

Illinois law provides that:

> Designation of Parties – "…(c) A party shall set forth in the body of his or her pleading the names of all parties for and against whom relief is sought thereby … (e) ***Upon application and for good cause shown the parties may appear under fictitious names.*** 735 ILCS 5/2-401.

The identification of "the parties to a proceeding is an important dimension of publicness [and] the public has a right to know who is utilizing the courts that its tax dollars support." *A.P. v. M.E.E.,* 354 Ill. App. 3d 989, 1003, 821 N.E.2d 1238 (1st Dist. 2004). In considering whether to allow an entity to proceed anonymously, a court must evaluate whether the person seeking to use a pseudonym has shown a privacy interest that outweighs the public's interest in judicial proceedings being open to the public. *Doe v. Doe,* 282 Ill. App. 3d 1078, 1088, 668 N.E.2d 1160 (1st Dist. 1996). In order to proceed anonymously, a person must show that his or her privacy interest is exceptional, and that it involves matters of a highly personal nature, such as matters relating to adoption, sexual orientation or religion. *Id.* Furthermore, the use of a fictitious name is permissible when necessary to protect the privacy of children, sexual assault victims and other types of particularly vulnerable parties or witnesses. *See A.P.*, 354 Ill. App. 3d at 1003.

Movant has failed to meet the high threshold for obtaining permission to proceed anonymously, and has failed to articulate any support in Illinois law suggesting that he has any exceptional privacy interest in not disclosing its identifying information, or that Petitioner is seeking any information of a highly personal nature that would allow it to continue to proceed anonymously. The Court should deny this request.

V. ARGUMENT REGARDING "SUBPOENA'S VERY INTENT" FAILS.

Movant's final argument in its "Motion to Quash" is that "[t]he subpoena is actually invalid on its face because" it seeks disclosure of information to Petitioner. This argument fails for two reasons.

First, there is no subpoena, a fact Movant persistently fails to recognize. As such, his argument is irrelevant. Furthermore, Movant's citation to a 1979 case for the proposition that documents responsive to a subpoena should be turned over to the Court, which in turn "determines the relevance and materiality of the subpoenaed materials," ignores the modern practice of law. Courts do not routinely review and respond to subpoenas for the benefit of litigants. This argument fails as well.

CONCLUSION

For all of the foregoing reasons, Petitioner respectfully requests that the Court deny the Motion, and grant Petitioner any and all further relief that the Court deems to be reasonable and appropriate under the circumstances.

Respectfully submitted,

GUAVA LLC

By: ______________________________
Paul A. Duffy, Esq.
Prenda Law, Inc.
161 N. Clark Street
Suite 3200
Chicago, IL 60601
Telephone: (312) 880-9160
Facsimile: (312) 893-5677
E-mail: paduffy@wefightpiracy.com
Attorney for Petitioner

By: ______________________________
Kevin T. Hoerner, Esq.
Becker, Paulson, Hoerner &
Thompson, P.C.
5111 West Main Street
Belleville, IL 62226
Telephone: (618) 235-0020
Attorney for Petitioner

Dated: February 12, 2013

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing instrument was served upon all counsel of record or movants in this cause via hand delivery and/or by enclosing same in an envelope addressed to such parties as indicated by the pleadings herein, with postage fully prepaid, and by depositing said envelope in a U.S. Post Office mail box in Belleville, Illinois on this 13th day of February, 2013.

EXHIBIT GG

EXHIBIT GG

I, Alan Mooney, being duly sworn, depose and state:

1. I am over the age of eighteen, suffer no legal disabilities, have personal knowledge of the facts set forth below, and am competent to testify.

2. On November 20, 2012, I executed a verification in a case captioned Guava LLC v. Comcast Cable Communications, LLC, which is currently pending in the Circuit Court of the Twentieth Judicial Circuit St. Clair County, Illinois (Case no. 12-mr-417).

3. I have been informed that questions have arisen as to the authenticity of the verification. I can attest that the verification is and was authentic and that the statements set forth the the petition continue to be accurate.

4. My company is suffering severe financial losses due to the criminal activity outlined in the petition and I believe it is my responsibility as a principal of Guava LLC to seek redress in the courts.

5. In order to put to rest the bizarre conspiracy theories raised by certain attorneys regarding my November 20, 2012 verification, I have taken the extra step of completing this affidavit and having a different notary authenticate my signature. I trust that the step of having now two independent notaries verify my identity will allow my attorneys to proceed in protecting my company from future harm.

STATE OF MINNESOTA

ss.

COUNTY OF Hennepin

The foregoing instrument was acknowledged before me this 15th day of February, 2013.

NOTARIAL STAMP OR SEAL (OR OTHER TITLE OR RANK)

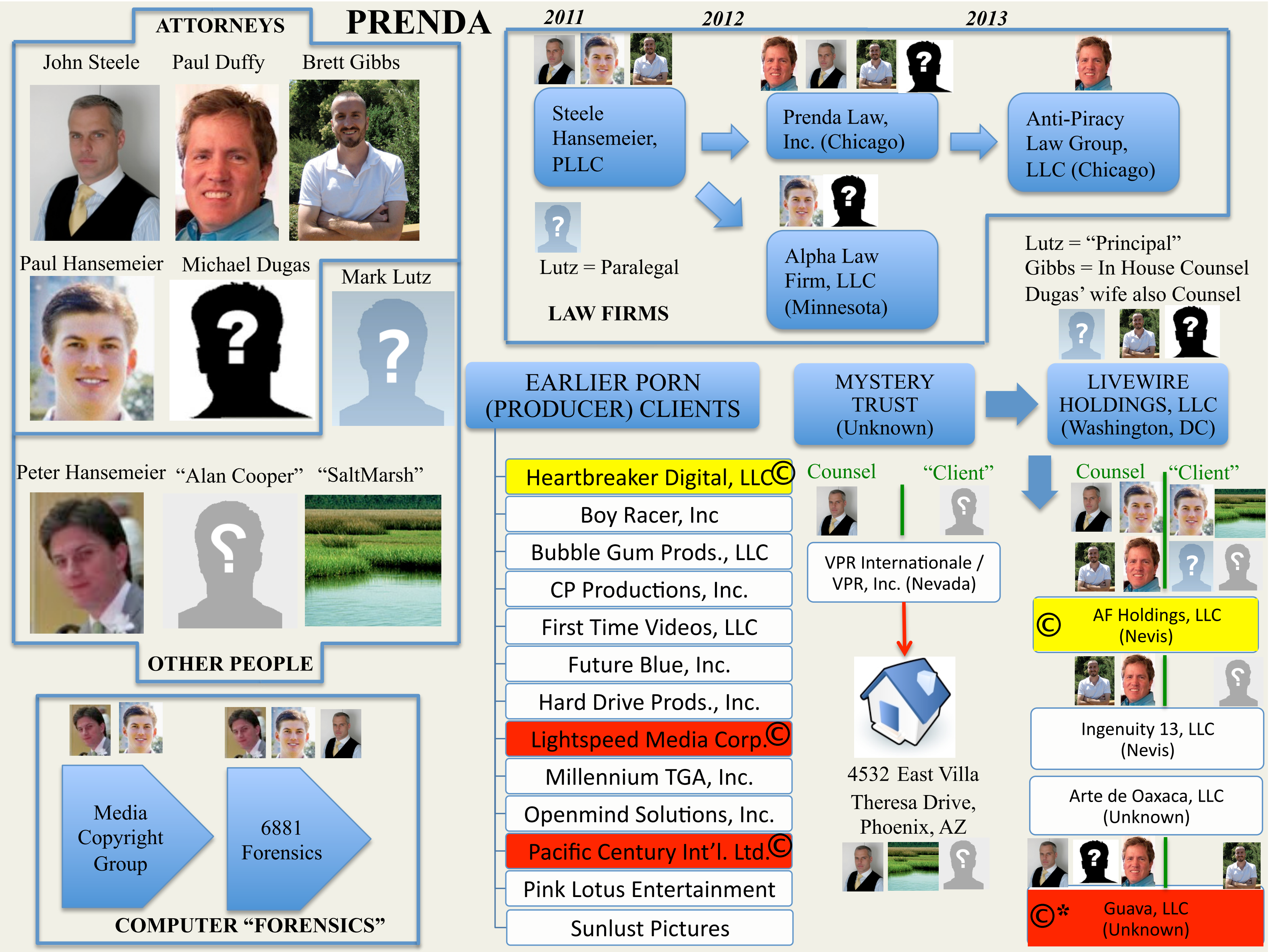
SIGNATURE OF NOTARY OR AUTHORIZED OFFICIAL

My Commission Expires: ____________________

ROBERT EDMUND JONES
NOTARY PUBLIC - MINNESOTA
MY COMMISSION EXPIRES 1/31/2015

EXHIBIT HH

EXHIBIT HH



PRENDA

ATTORNEYS

John Steele

Paul Duffy

Brett Gibbs

Paul Hansemeier

Michael Dugas

Mark Lutz

OTHER PEOPLE

Peter Hansemeier

“Alan Cooper”

“SaltMarsh”

COMPUTER “FORENSICS”

Media Copyright Group

6881 Forensics

LAW FIRMS

2011

2012

2013

Steele Hansemeier, PLLC

Prenda Law, Inc. (Chicago)

Anti-Piracy Law Group, LLC (Chicago)

Alpha Law Firm, LLC (Minnesota)

Lutz = Paralegal

Lutz = “Principal”
Gibbs = In House Counsel
Dugas’ wife also Counsel

EARLIER PORN (PRODUCER) CLIENTS

- Heartbreaker Digital, LLC ©
- Boy Racer, Inc
- Bubble Gum Prods., LLC
- CP Productions, Inc.
- First Time Videos, LLC
- Future Blue, Inc.
- Hard Drive Prods., Inc.
- Lightspeed Media Corp. ©
- Millennium TGA, Inc.
- Openmind Solutions, Inc.
- Pacific Century Int’l. Ltd. ©
- Pink Lotus Entertainment
- Sunlust Pictures

MYSTERY TRUST (Unknown)

Counsel

“Client”

VPR Internationale / VPR, Inc. (Nevada)

4532 East Villa Theresa Drive, Phoenix, AZ

LIVEWIRE HOLDINGS, LLC (Washington, DC)

Counsel

“Client”

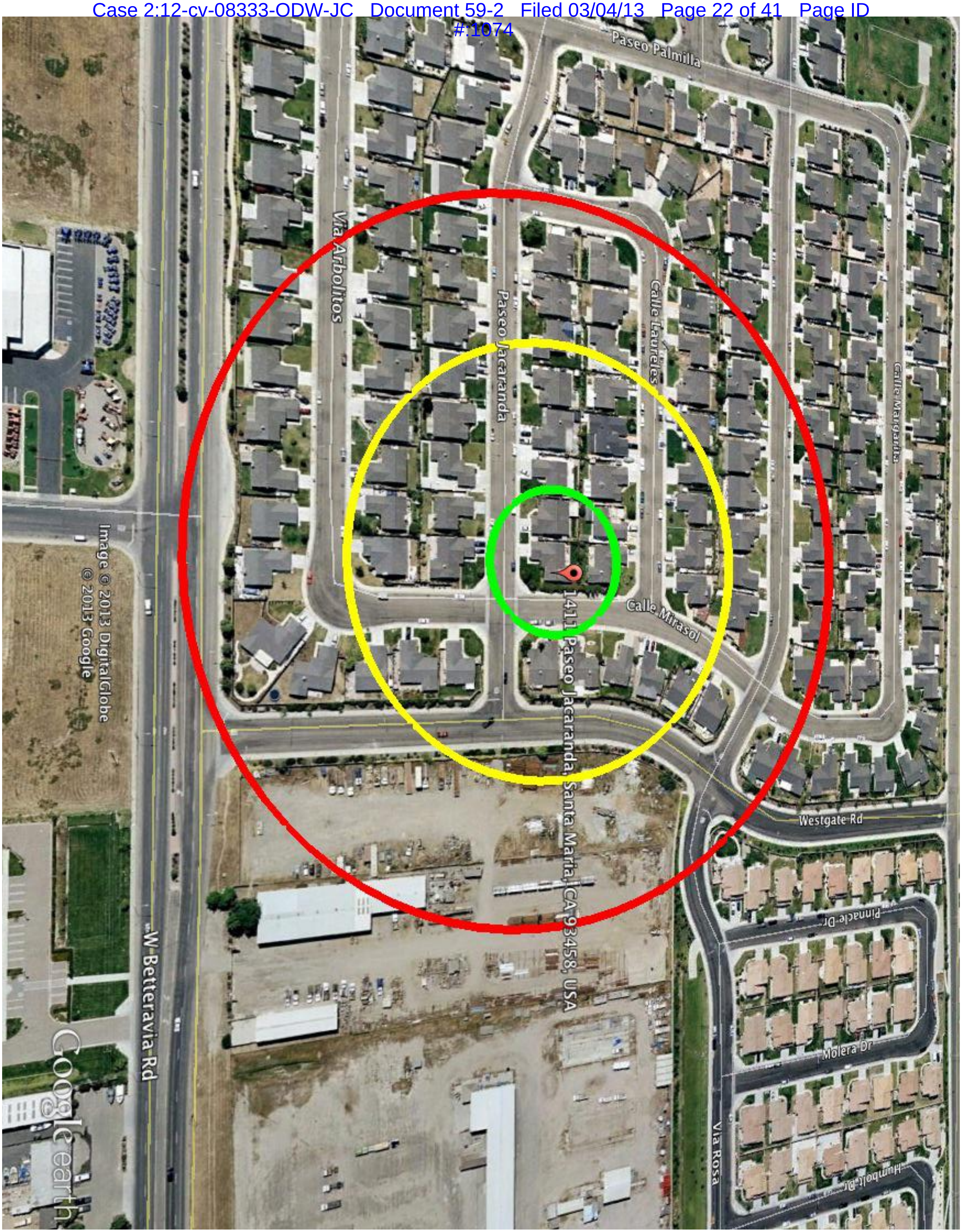
© AF Holdings, LLC (Nevis)

Ingenuity 13, LLC (Nevis)

Arte de Oaxaca, LLC (Unknown)

©* Guava, LLC (Unknown)

EXHIBIT II


Paseo Palmilla
Via Arbolitos
Paseo Jacaranda
Calle Laureles
Calle Margarita
Calle Mirasol
1411 Paseo Jacaranda, Santa Maria, CA 93458, USA
Westgate Rd
Pinnacle Dr
Molera Dr
Via Rosa
Humbolt Dr
W Betteravia Rd
Image © 2013 DigitalGlobe
© 2013 Google
Google earth

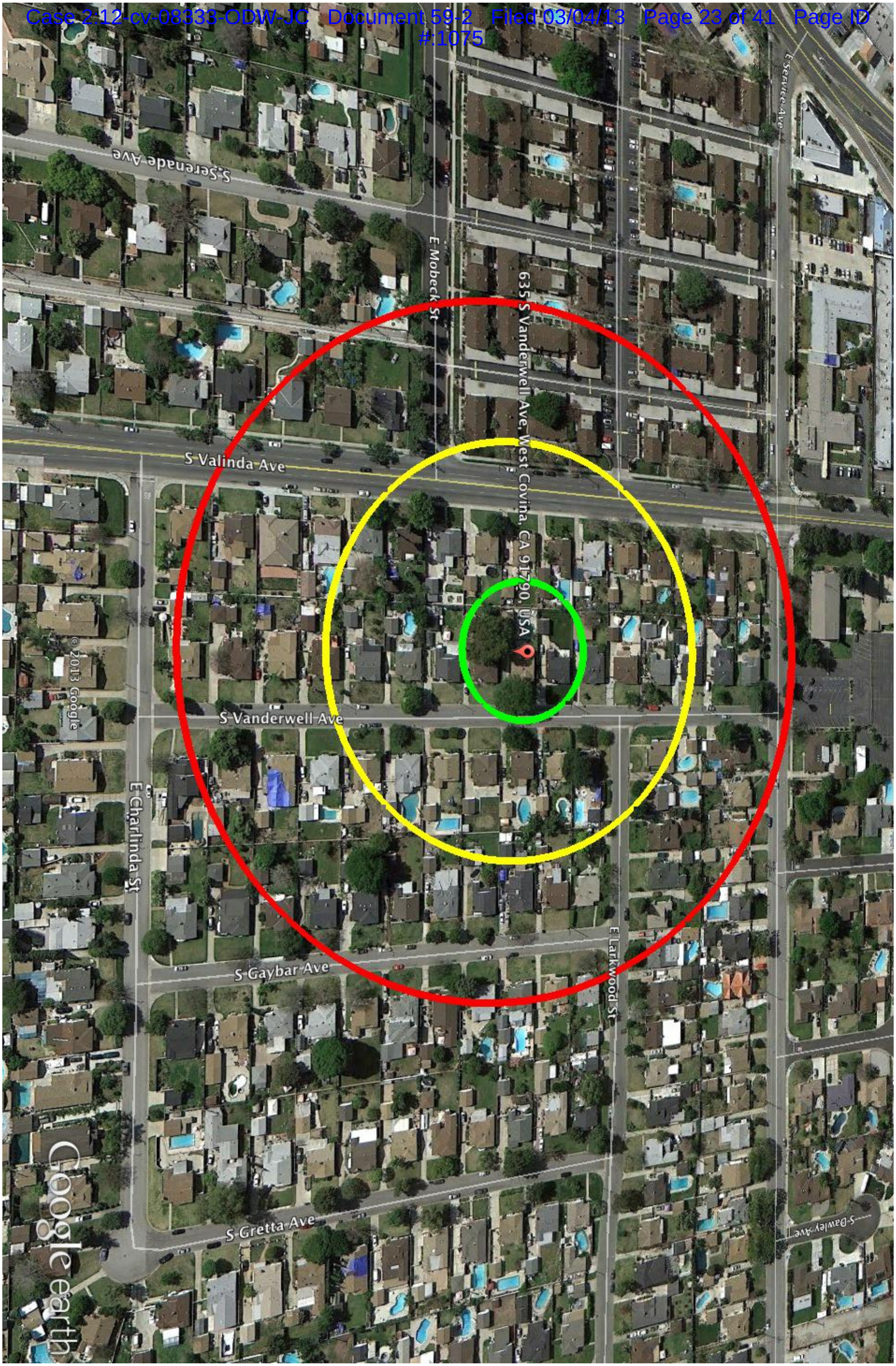

S Serenade Ave
E Service Ave
E Mobeck St
635 S Vanderwell Ave, West Covina, CA 91790, USA
S Valinda Ave
© 2013 Google
S Vanderwell Ave
E Charlinda St
E Larkwood St
S Gaybar Ave
S Gretta Ave
S Dawley Ave
Google earth

EXHIBIT JJ

Reference Manual for the 108 Mbps Wireless Firewall Router WGT624

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

M-10153-01
Version 1.0
August 2003

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

1. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

Europe - EU Declaration of Conformity

CE 0984 (!)	This device is a 2.4 GHz low power RF device intended for home and office use in EU and EFTA member states. In some EU / EFTA member states some restrictions may apply. Please contact local spectrum management authorities for further details before putting this device into operation.

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950, EN 60950 1992 2nd Edition (A1-A4, A11) Safety of Information Technology Equipment, Including Electrical Business Equipment EN 300 328-1 V1.3.1 (2001-12); EN 300328-2 V1.2.1 (2001-12) Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission system; data transmission equipment operating in the 2.4 Ghz ISM band and using spread spectrum modulation techniques; Part 1: Technical characteristics and test conditions; Part 2; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.

EN 301 489-1, Aug. 2000; EN 301489-17, Sept. 2000 - Electromagnetic compatibility and radio spectrum matters (ERM); electromagnetic compatibility (EMC); standard for radio equipment and services: Part 1: Common technical requirements; Part 17: Specific conditions for Wideband Data and Hiperlan equipment.

EN 55 022 Declaration of Conformance

This is to certify that the 108 Mbps Wireless Firewall Router WGT624 is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Compliance with the applicable regulations is dependent upon the use of shielded cables. It is the responsibility of the user to procure the appropriate cables.

Requirements For Operation in the European Community

Countries of Operation and Conditions of Use in the European Community

The user should run the configuration utility program provided with this product to check the current channel of operation and confirm that the device is operating in conformance with the spectrum usage rules for European Community countries as described in this section. European standards dictate a maximum radiated transmit power of 100mW EIRP and a frequency range of 2.400 - 2.4835 Ghz.

Operation Using 2.4 GHz Channels in France

The following radio channel usage limitations apply in France.

The radio spectrum regulator in France, Autorité de regulation des telecommunications (ART), enforces the following rules with respect to use of 2.4GHz spectrum in various locations in France. Please check ART's web site for latest requirements for use of the 2.4GHz band in France: http://www.art-telecom.fr/eng/index.htm. When operating in France, this device may be operated under the following conditions:

Indoors only, using any channel in the 2.4465-2.4835 GHz band.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 108 Mbps Wireless Firewall Router WGT624 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the 108 Mbps Wireless Firewall Router WGT624 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your 108 Mbps Wireless Firewall Router WGT624.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a web browser such as Internet Explorer or Netscape are required.

Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your WGT624 wireless router. In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your firewall in order to maximize the network speed. For further information on wireless networking, refer to in Appendix D, "Wireless Networking Basics.

Observe Performance, Placement, and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless firewall. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

> **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range/ performance specifications, please see Appendix A, "Technical Specifications."

For best results, place your firewall:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook PC.

Implement Appropriate Wireless Security

➡	**Note:** Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 500 feet. Such distances can allow for others outside of your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WGT624 wireless router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

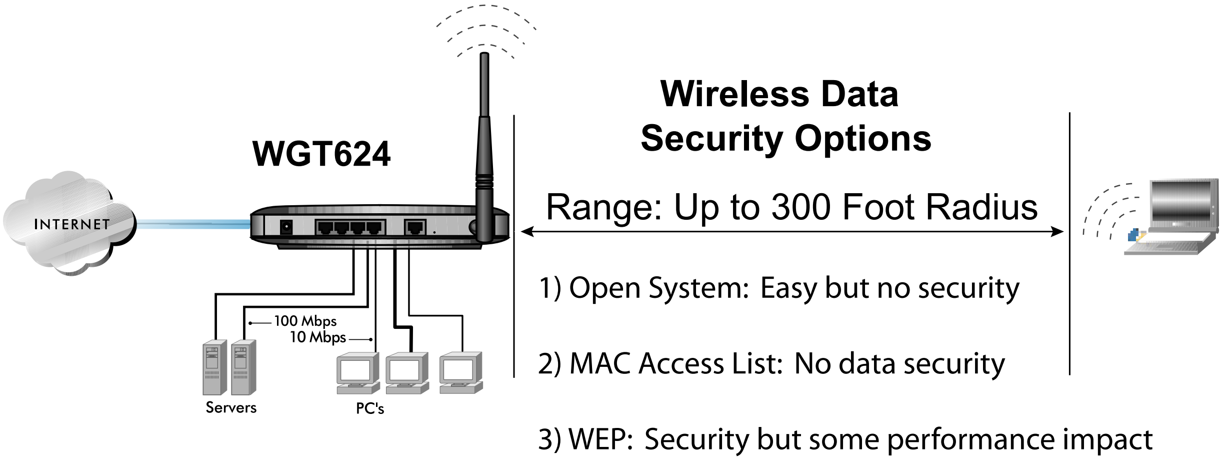

WGT624
INTERNET
100 Mbps
10 Mbps
Servers
PC's
Wireless Data Security Options
Range: Up to 300 Foot Radius
1) Open System: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but some performance impact

Figure 4-1: WGT624 wireless data security options

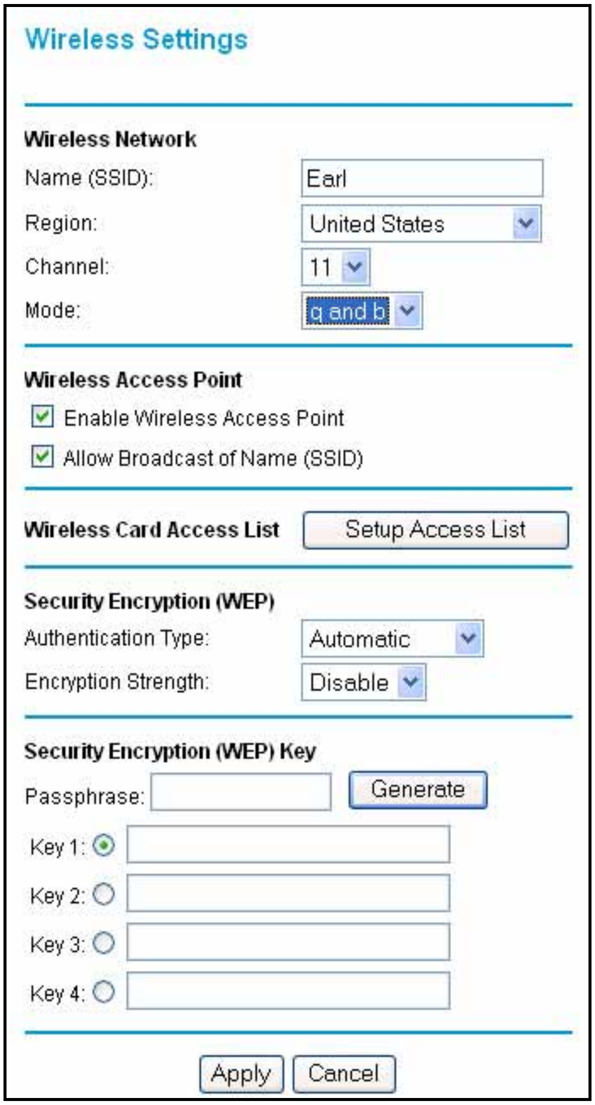
There are several ways you can enhance the security of you wireless network.

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs o that unknown PCs cannot wirelessly connect to the WGT624. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

- **Turn Off the Wired LAN.** If you disable the wireless LAN, wireless devices cannot communicate with the router at all. You might choose to turn off the wireless the LAN when you are away and the others in the household all use wired connections.

Understanding Wireless Settings

To configure the Wireless settings of your firewall, click the Wireless link in the main menu of the browser interface. The Wireless Settings menu will appear, as shown below.



Wireless Settings

Wireless Network

Name (SSID): Earl

Region: United States

Channel: 11

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Card Access List

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: Disable

Security Encryption (WEP) Key

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Figure 4-2: Wireless Settings menu

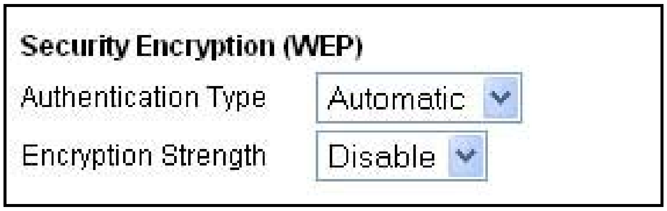
The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion.

- **Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use this SSID for that network. The WGT624 default SSID is: **NETGEAR**.
- **Region.** This field identifies the region where the WGT624 can be used. It may not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.
- **Channel.** This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page D-7.
- **Mode.** This field determines which data communications protocol will be used. You can select "g only," 108 Mbps Turbo g only, or "g and b." "g only" dedicates the WGT624 to communicating with the higher bandwidth 802.11g wireless devices exclusively. The "g and b" mode provides backward compatibility with the slower 802.11b wireless devices while still enabling 802.11g communications. The 108 Mbps Turbo mode only works with other 802.11g turbo devices that support this turbo mode.
- **Allow Broadcast of Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network 'discovery' feature of some products such as Windows XP.
- **Enable Wireless Access Point.** If you disable the wireless access point, wireless devices cannot connect to the WGT624.
- **Wireless Card Access List.** When the Trusted PCs Only radio button is selected, the WGT624 checks the MAC address of the wireless station and only allows connections to PCs identified on the trusted PCs list.

Understanding WEP Authentication and Encryption

Restricting wireless access to your network prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEB data encryption settings described below will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a web site is using SSL because the web address begins with HTTPS rather than HTTP.

Authentication Scheme Selection



Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: Disable

Figure 4-3: Encryption Strength

The WGT624 lets you select the following wireless authentication schemes.

- Automatic.
- Open System.
- Shared key.

> ➡ **Note:** The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

Be sure to set your wireless adapter according to the authentication scheme you choose for the WGT624 wireless router. Please refer to "Authentication and WEP" on page D-3 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

Encryption Strength Choices

Choose the encryption strength from the drop-down list. Please refer to "Overview of WEP Parameters" on page D-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

- **Disable.** No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.
- **64-bit or 128-bit WEP.** When 64-bit or 128-bit is selected, WEP encryption will be applied.

If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and access points in your network.

There are two methods for creating WEP encryption keys:

- **Passphrase**. Enter a word or group of printable characters in the Passphrase box and click the Generate button. These characters *are* case sensitive.
- **Manual**. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). These values *are not* case sensitive.

Default Factory Settings

When you first receive your WGT624, the default factory settings are shown below. You can restore these defaults with the Factory Default Restore button on the rear panel. After you install the WGT624 wireless router, use the procedures below to customize any of the settings to better meet your networking needs.

FEATURE	DEFAULT FACTORY SETTINGS
Wireless Access Point	**Enabled**
Wireless Access List (MAC Filtering)	**All wireless stations allowed**
SSID broadcast	**Enabled**
SSID	**NETGEAR**
11b/g RF Channel	**11**
Mode	**g and b**
Authentication Type	**Open System**
WEP	**Disabled**

Before You Change the SSID and WEP Settings

Before customizing your wireless settings, print this form and record the following information. If your working with an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Otherwise, you will choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces below.

- **Network Name (SSID)*:*** The Service Set Identification (SSID), called the wireless network name in Windows XP, identifies the wireless network. You may use up to 32 alphanumeric characters. Record your customized SSID on the line below.

  Name (SSID):________________________________

  Note: The SSID in the wireless router is the SSID you configure in the wireless adapter card. For the access point and wireless nodes to communicate with each other, all must be configured with the same SSID.

- **Authentication.** The authentication setting, “Open System” or “Shared Key,” is unrelated to encryption of transmissions. The two bands can use different authentication settings. Choose “Shared Key” for more security, circle one: Open System or Shared Key

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well.

- **WEP Encryption Strength**. Choose the key size. Circle one: **64** or **128** bits.

- **WEP Encryption Keys**. The WGT624 provides two methods for creating WEP encryption keys:

  – **Passphrase**. ________________________________ Enter a word or group of printable characters. These characters *are* case sensitive. When you enter the Passphrase and click the Generate button on the WGT624, the keys will be generated.

  – **Manual**. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0-9 or a-f). These values *are not* case sensitive. For 128-bit WEP, enter 26 hexadecimal digits.

  Whichever method you use, record the key values in the spaces below.

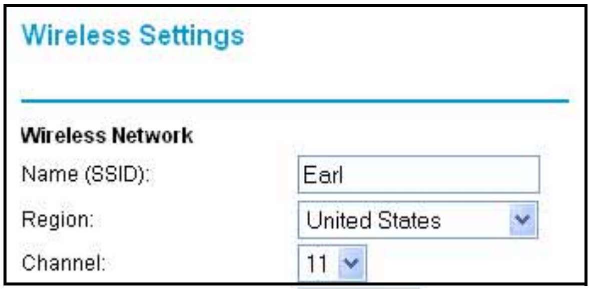
  Key 1: ______________________________________
  Key 2: ______________________________________
  Key 3: ______________________________________
  Key 4: ______________________________________

Use the procedures described in the following sections to configure the WGT624. Store this information in a safe place.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the WGT624 firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the WGT624 firewall.



Wireless Settings

Wireless Network

Name (SSID): Earl

Region: United States

Channel: 11

Figure 4-4: Wireless Settings menu

3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

   Note: The SSID of any wireless access adapters must match the SSID you configure in the 108 Mbps Wireless Firewall Router WGT624. If they do not match, you will not get a wireless connection to the WGT624.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the Channel. The default channel is 11.

   This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your firewall. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page D-7.

6. For initial configuration and test, leave the Wireless Card Access List set to "Everyone" and the Encryption Strength set to "Disabled."
7. Click Apply to save your changes.

➡	**Note:** If you are configuring the firewall from a wireless PC and you change the firewall's SSID, channel, or security settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your PC to match the firewall's new settings.

8. Configure and test your PCs for wireless connectivity.

   Program the wireless adapter of your PCs to have the same SSID and channel that you configured in the router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the firewall.

Once your PCs have basic wireless connectivity to the firewall, then you can configure the advanced wireless security functions of the firewall.

How to Restrict Wireless Access by MAC Address

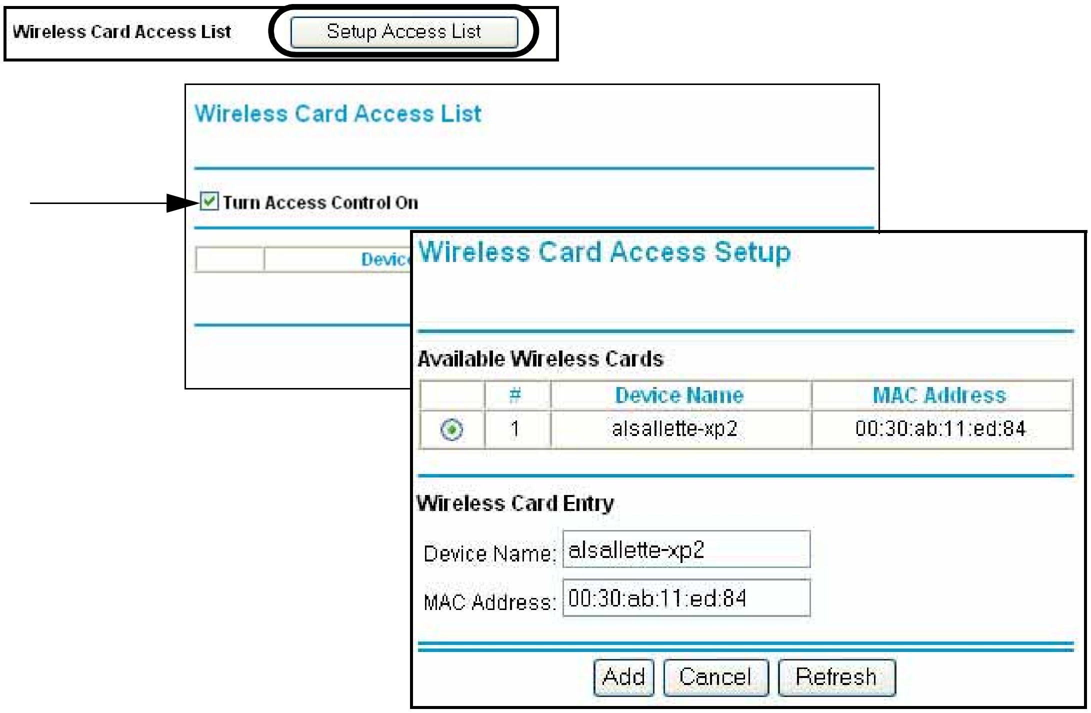
To restrict access based on MAC addresses, follow these steps:

1. Log in to the WGT624 firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

➡	**Note:** When configuring the firewall from a wireless PC whose MAC address is not in the Trusted PC list, if you select Turn Access Control On, you will lose your wireless connection when you click on Apply. You must then access the wireless router from a wired PC or from a wireless PC which is on the access control list to make any further changes.

2. Click the Wireless Settings link in the main menu of the WGT624 firewall.

3. From the Wireless Settings menu, click the Setup Access List button to display the Wireless Access menu shown below.



☑ Turn Access Control On

	#	Device Name	MAC Address
●	1	alsallette-xp2	00:30:ab:11:ed:84

Device Name: alsallette-xp2

MAC Address: 00:30:ab:11:ed:84

Figure 4-5: Wireless Card Access List Setup

4. Click Add to add a wireless device to the wireless access control list. The Available Wireless Cards list displays.
5. Click the Turn Access Control On check box.
6. Then, either select from the list of available wireless cards the WGT624 has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.

   Note: You can copy and paste the MAC addresses from the firewall's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless PC to obtain a wireless link to the firewall. The PC should then appear in the Attached Devices menu.
7. Click Add to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen. Repeat these steps for each additional device you wish to add to the list.
8. Be sure to click Apply to save your wireless access control list settings.

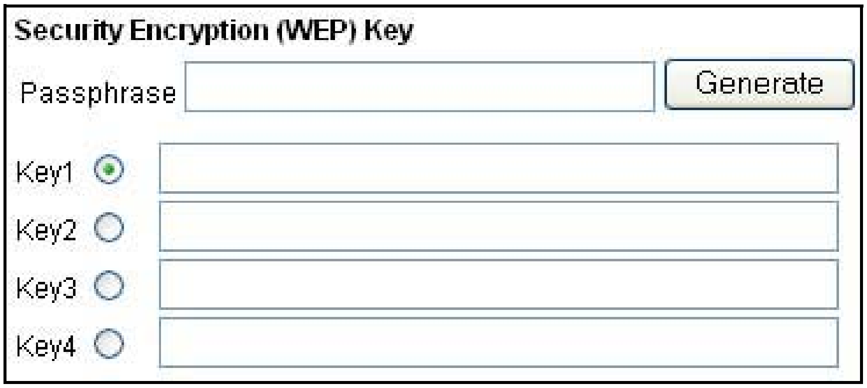
Now, only devices on this list will be allowed to wirelessly connect to the WGT624.

How to Configure WEP

To configure WEP data encryption, follow these steps:

➡	**Note:** If you use a wireless PC configure WEP settings, you will be disconnected when you click on Apply. You must then either configure your wireless adapter to match the wireless router WEP settings or access the wireless router from a wired PC to make any further changes.

1. Log in to the WGT624 firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the WGT624 firewall.
3. From the Security Encryption menu drop-down list, select the WEP encryption strength you will use.



Security Encryption (WEP) Key

Passphrase [ ] Generate

Key1 ●

Key2 ○

Key3 ○

Key4 ○

Figure 4-6. Wireless Settings encryption menu

4. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
   - Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
   - Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F) Select which of the four keys will be active.

   Please refer to "Overview of WEP Parameters" on page D-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.
5. Click Apply to save your settings.