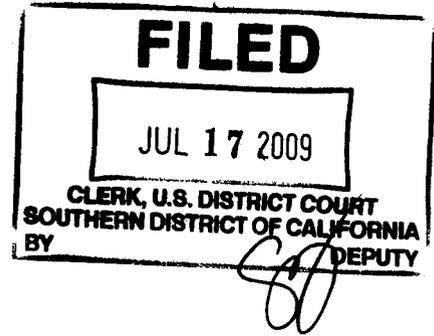


1 MARK J. HATTAM (BAR NO. 173667)
2 MICHAEL J. HOLMES (BAR NO. 199311)
3 ALLEN MATKINS LECK GAMBLE
4 MALLORY & NATSIS LLP
5 501 West Broadway, 15th Floor
6 San Diego, California 92101-3541
7 Phone: (619) 233-1155
8 Fax: (619) 233-1158
9 E-Mail: mhattam@allenmatkins.com
10 mholmes@allenmatkins.com



11 CHAD M. HAGAN (PRO HAC VICE PENDING)
12 DAVID M. NOLL (PRO HAC VICE PENDING)
13 CLAYTON D. CRAIGHEAD (PRO HAC VICE PENDING)
14 HAGAN NOLL & BOYLE LLC
15 820 Gessner, Suite 940
16 Houston, TX 77024
17 Phone: (713) 343-0478
18 Fax: (713) 758-0146
19 E-Mail: chad.hagan@hnbllc.com
20 david.noll@hnbllc.com
21 clayton.craighead@hnbllc.com

22 Attorneys for Plaintiffs

23 UNITED STATES DISTRICT COURT
24 SOUTHERN DISTRICT OF CALIFORNIA

25 DISH NETWORK L.L.C., a Colorado Limited
26 Liability Company, ECHOSTAR
27 TECHNOLOGIES L.L.C., a Texas Limited
28 Liability Company, and NAGRASTAR L.L.C.,
a Colorado Limited Liability Company,

Plaintiffs,

v.

29 SONICVIEW USA, INC., a California
30 Corporation, SONICVIEWRA LLC, a
31 California Limited Liability Company,
32 SONICVIEWSA LLC, a California Limited
33 Liability Company, ROBERTO SANZ,
34 individually, DONTPAY4TV, LLC, a
35 California Limited Liability Company, DUANE
36 BERNARD, individually, COURTNEY
37 BERNARD, individually, and DOES 1-50,

Defendants.

Case No. '09 CV 1 553 H NLS

PLAINTIFFS' COMPLAINT FOR:

- 1) VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, 17 U.S.C. § 1201(a)(1);
- 2) VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, 17 U.S.C. § 1201(a)(2);
- 3) VIOLATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, 17 U.S.C. § 1201(b)(1);
- 4) VIOLATION OF THE COMMUNICATIONS ACT OF 1934, AS AMENDED, 47 U.S.C. § 605(a);
- 5) VIOLATION OF THE COMMUNICATIONS ACT OF 1934, AS AMENDED, 47 U.S.C. § 605(e)(4);
- 6) VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. § 2511(1)(a)

1 Plaintiffs, DISH Network, L.L.C. ("DISH Network"), EchoStar Technologies, L.L.C.
2 ("EchoStar"), and NagraStar, L.L.C., ("NagraStar") (collectively "DISH Network" or "Plaintiffs"),
3 by their undersigned counsel, file this Original Complaint against the above-named Defendants
4 and state as follows:

5 **INTRODUCTION & NATURE OF THE ACTION**

6 1. Plaintiffs bring this action against Defendants Sonicview USA, Inc., Sonicviewra
7 LLC, Sonicviewsa LLC, Roberto Sanz, DontPay4TV, LLC, Duane Bernard, Courtney Bernard,
8 and DOES 1-50, (collectively "Defendants") for unlawfully manufacturing, distributing, and
9 otherwise trafficking in devices, components, and technologies intended to facilitate the illegal and
10 unauthorized reception and decryption of DISH Network's satellite television programming
11 ("DISH Network Programming").

12 2. DISH Network is a multi-channel video provider, providing video, audio, and data
13 services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a
14 Direct Broadcast Satellite system. DISH Network uses satellites to broadcast, among other things,
15 movies, sports, and general entertainment services to consumers who have been authorized to
16 receive such services after payment of a subscription fee (or in the case of a pay-per-view movie
17 or event, the purchase price).

18 3. To provide customers with a variety of programming channels, DISH Network
19 continues to contract with and purchase the distribution rights of copyrighted programming from
20 network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors,
21 sports leagues, event promoters, and other content providers, including HBO, SHOWTIME,
22 ESPN, Cinemax, and Disney.

23 4. Because DISH Network generates revenues through the sale of subscription
24 packages and pay-per-view programming, and because the ability to attract and retain distribution
25 rights for programming is dependent upon preventing unauthorized reception of DISH Network
26 Programming, DISH Network's video channels, except for certain promotional channels, are all
27 digitally secured and encrypted.

28

1 5. Plaintiffs protect their DISH Network Programming from unauthorized viewing by
2 using a management and security system ("Security System"), which serves two interrelated
3 functions: (1) subscriber-management—allowing DISH Network to "turn on" or "turn off"
4 Programming that a customer ordered, cancelled, or changed; and (2) encryption—preventing
5 individuals or entities who have not purchased DISH Network Programming from viewing it.

6 6. The Security System is comprised of two parts. First, DISH Network encrypts
7 (electronically scrambles) its satellite signals using proprietary technology provided by NagraStar.
8 Essentially, NagraStar provides DISH Network with "smart cards" ("Access Cards") that contain a
9 microprocessor component that functions as a security computer to a "conditional access system"
10 known as Digital Nagra Advanced Security Process ("DNASP"). These Access Cards and related
11 encryption technology are utilized in the satellite receivers that customers either purchase or lease.
12 Second, the DNASP uses a complex encryption system that is combined with a Digital Video
13 Broadcasting ("DVB") scrambler/encoding system to effectively protect and encrypt DISH
14 Network Programming.

15 7. Defendants violated federal and state law by manufacturing, offering to the public,
16 providing, or otherwise engaging in the traffic of devices, components, and technology that are
17 primarily designed to circumvent and/or defeat Plaintiffs' Security System and ultimately facilitate
18 the unauthorized reception of Plaintiffs' encrypted satellite signals and copyrighted DISH Network
19 Programming.

20 **PARTIES**¹

21 8. Plaintiff DISH Network L.L.C. is a Colorado limited liability company with its
22 principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112,
23 Arapahoe County. Plaintiff DISH Network L.L.C.'s sole member is DISH DBS Corporation, a
24 Colorado Corporation, which in turn is an indirect wholly owned subsidiary of DISH Network
25

26 ¹ DISH Network's allegations related to the wrongful conduct of Defendants are based upon the
27 investigation and device analysis DISH Network has completed to date, upon information and
28 belief, and with the reasonable belief that further investigation and discovery in this action will
lead to additional factual support. DISH Network therefore expressly reserves its right to
supplement, amend and/or otherwise modify its claims and the basis thereof, as additional
investigation and discovery is conducted.

1 Corporation, a Nevada Corporation. DISH Network Corporation is publicly owned and traded on
2 the NASDAQ national market under the symbol "DISH."

3 9. Plaintiff EchoStar Technologies L.L.C. is a Texas limited liability company with its
4 principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112,
5 Arapahoe County. Plaintiff EchoStar Technologies L.L.C.'s sole member is EchoStar
6 Corporation, a Nevada Corporation. EchoStar Corporation is publicly owned and traded on the
7 NASDAQ national market under the symbol "SATS."

8 10. Plaintiff NagraStar L.L.C. is a Colorado limited liability company with its principal
9 place of business located at 90 Inverness Circle East, Englewood, Colorado 80112, Arapahoe
10 County. NagraStar is a joint venture between EchoStar Corporation and the Kudelski Group, a
11 group of companies headquartered in Switzerland. Plaintiff NagraStar L.L.C.'s sole members are
12 EchoStar Corporation and Kudelski SA. EchoStar Corporation is identified in paragraph 11
13 above. Kudelski SA has its principal place of business at 22-24, Route de Genève, 1033
14 Cheseaux, Switzerland and is listed on the SIX Swiss Exchange under the symbol "KUD."

15 11. Defendant Sonicview USA, Inc. is a California corporation, Sonicviewra LLC is a
16 California limited liability company, Sonicviewsa LLC is a California limited liability company
17 (collectively "Sonicview"), with their principal place of business located at 1730 Ord Way,
18 Oceanside, CA 92056 and 1732 Ord Way, Oceanside, CA 92056. The registered agent for
19 Sonicview USA Inc. is Roberto Sanz, 9930 Mollie Lane, Santee, CA 92071. The registered agent
20 for Sonicviewra LLC is Roberto Sanz, 843 Sumac Pl., Escondido, CA 92027. The registered
21 agent for Sonicviewsa LLC is Roberto Sanz, 1732 Ord Way, Oceanside, CA 92056. Sonicview
22 sells and distributes numerous pirate devices including Sonicview satellite television receivers,
23 Sonicview I-Hubs, and pirate software. Sonicview sells and distributes devices known as Sub-
24 Boards, Q-Boards, and A-1 Boards (collectively "8PSK Turbo Boards"). Sonicview also
25 distributes pirate software through the website, www.ftalife.com. Sonicview operates the Xtraba
26 storefront at 1100 N. Magnolia, Suites I and J, El Cajon, CA 92020.

27 12. Defendant Roberto Sanz is an individual residing at 6137 Castilla St., Santee,
28 California 92071. Roberto Sanz is owner and operator of Sonicview. Roberto Sanz operates

1 numerous websites including www.extremesats.com and www.kingsatellite.com whereupon he
2 sells and distributes Sonicview receivers, Sonicview I-Hubs, 8PSK Turbo Boards. Roberto Sanz
3 also distributes pirate software through the website, www.ftalife.com. Roberto Sanz operates the
4 Xtraba storefront at 1100 N. Magnolia, Suites I and J, El Cajon, CA 92020.

5 13. Defendant DontPay4TV, LLC ("DontPay4TV") is a California limited liability
6 company with its principal place of business located at 1100 N. Magnolia Ave., Suite I, El Cajon,
7 CA 92020 and 1100 N. Magnolia Ave., Suite J, El Cajon, CA 92020. The registered agent for
8 DontPay4TV is Duane Bernard, 9640b Mission Gorge Rd #237, Santee, CA 92071. DontPay4TV
9 sells and distributes Sonicview receivers, 8PSK Turbo Boards, Sonicview I-Hubs through various
10 websites including www.megadropshippers.com. DontPay4TV also distributes pirate software
11 through the website, www.ftalife.com. DontPay4TV operates the Xtraba storefront at 1100 N.
12 Magnolia, Suites I and J, El Cajon, CA 92020.

13 14. Defendant Duane Bernard is an individual residing in San Diego, California.
14 Duane Bernard is owner and operator of DontPay4TV. Duane Bernard is a business partner of
15 Roberto Sanz. Duane Bernard sells and distributes Sonicview receivers, 8PSK Turbo Boards,
16 Sonicview I-Hubs through various websites including www.megadropshippers.com and
17 www.xtraba.com. Duane Bernard also distributes pirate software through the website,
18 www.ftalife.com. Duane Bernard operates the Xtraba storefront at 1100 N. Magnolia, Suites I and
19 J, El Cajon, CA 92020.

20 15. Defendant Courtney Bernard is an individual residing in San Diego, California.
21 Courtney Bernard sells and distributes Sonicview receivers, 8PSK Turbo Boards, Sonicview I-
22 Hubs through various websites including www.xtraba.com. Courtney Bernard also distributes
23 pirate software through the website, www.ftalife.com. Courtney Bernard operates the Xtraba
24 storefront at 1100 N. Magnolia, Suites I and J, El Cajon, CA 92020.

25 16. The true names and capacities of Defendants DOES 1 through 50, whether
26 individual, corporate, associate, or otherwise, are currently unknown to Plaintiffs at this time for
27 certain reasons including their identities being masked by monikers used on the Internet and
28

1 through the use of proxy domain registrations. Plaintiffs believe that information obtained in
2 discovery will lead to the identification of each Defendant's true name.

3 17. Each of the Defendants, including DOES 1 through 50, was the agent and/or
4 principal for one another, was acting within the scope of such agency when engaging in the
5 misconduct alleged herein and/or otherwise acting on behalf of and/or in concert with each other,
6 and is jointly and severally liable for all damages arising as a result thereof.

7 18. Any judgment pursuant to Plaintiffs' request for relief should be rendered joint and
8 several against Defendants Sonicview USA, Inc. Sonicviewra LLC, Sonicviewsa LLC, Roberto
9 Sanz, DontPay4TV, LLC, Duane Bernard and Courtney Bernard.

10 **JURISDICTION AND VENUE**

11 19. This is a civil action predicated upon violations of the Digital Millennium
12 Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Communications Act of 1934, as amended, 47 U.S.C.
13 § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.*
14 Therefore, jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331, 1338, 47 U.S.C. §
15 605(e)(3)(A), 17 U.S.C. § 1203, and 18 U.S.C. § 2520(a).

16 20. Personal jurisdiction and venue are proper in this Court pursuant to 28 U.S.C. §§
17 1391(b)(1) because at least one Defendant resides within this judicial district and the remaining
18 Defendants reside in California, 1391(b)(2) because a substantial part of the events giving rise to
19 this action occurred in this judicial district, 1391(b)(3) because Defendants may be found in this
20 judicial district and are subject to *in personam* jurisdiction, and 1400(a) because this case asserts
21 the infringement and circumvention of protected copyright materials.

22 **PLAINTIFFS' SECURITY SYSTEM**

23 21. A consumer wishing to subscribe to and receive DISH Network Programming must
24 first have the necessary equipment which consists primarily of: a satellite dish; an integrated
25 receiver/decoder; and a credit card-sized DISH Network Access Card that is loaded into the
26 receiver through a slot on the face of the receiver. In certain more recent receiver models, referred
27 to as "cardless receivers," an internalized chip functions as an embedded Access Card.

28

1 22. The satellite dish is mounted at the subscriber's home or business. After proper
2 installation, the satellite dish will receive programming signals from one of DISH Network's
3 satellites. The receiver processes and descrambles the incoming signal using the data and
4 encryption technology stored in the DISH Network Access Card.

5 23. DISH Network provides its Access Cards to customers for use with the receivers
6 for the purpose of enabling authorized access to DISH Network Programming. Absent a
7 subscription, DISH Network will not provide a consumer an Access Card or authorize access to
8 encrypted DISH Network Programming. Subscribers are not authorized to modify or tamper with
9 the Access Card, which are clearly marked as property of DISH Network and must be returned
10 upon request.

11 24. The DISH Network Access Card is essential to the operation of the receiver
12 because it contains a secure embedded microprocessor that essentially functions as a security
13 computer, with proprietary keys and software that contain technology codes ("Nagra Software")
14 used to communicate with the receiver and descramble DISH Network Programming. Nagra
15 Software is licensed from Plaintiff NagraStar.

16 25. The Nagra Software within each DISH Network Access Card is supported by two
17 code segments of memory: Read-Only-Memory ("ROM"); and Electronically Erasable
18 Programmable Read-Only-Memory ("EEPROM"). Generally, the ROM code segment contains
19 the intimate knowledge and information regarding Plaintiffs' Security System and how it works;
20 whereas the EEPROM code segment contains the secret keys enabling the decryption of DISH
21 Network Programming.

22 26. The ROM code segment provides detailed instructions and commands to DISH
23 Network Access Cards and receivers in the normal operation of Plaintiffs' Security System.
24 Access to the proprietary information stored in the ROM code is necessary to unlock the safe
25 containing the secrets to Plaintiffs' Security System.

26 27. The EEPROM code segment stores data and command codes that have been
27 written to DISH Network Access Cards which the ROM code reads from to perform its calculation
28 and operation functions. Moreover, the EEPROM code segment contains secret keys including,

1 but not limited to "transmission" keys and "pairing" keys (collectively known as "Security
2 Keys"). The Security Keys are used, *inter alia*, to encrypt and decrypt the communications
3 between the DISH Network Access Card and the receiver. In addition, the Security System also
4 includes the IDEA algorithm (a patent on which is assigned to one of Plaintiff NagraStar's parent
5 companies and licensed to NagraStar for use in DISH Network's Security System).

6 28. DISH Network communicates with the microprocessor in each Access Card by
7 sending and receiving satellite signals which are routinely updated. The information transmitted
8 to and temporarily stored on the Access Card includes the most recent Security Keys and software
9 necessary to view DISH Network Programming.

10 29. Plaintiffs' Security System effectively controls access to the copyrighted materials
11 that comprise DISH Network Programming. In addition, the Security System ensures that the
12 protection afforded to such copyrighted works, such as limitations on the dissemination and use in
13 accordance with DISH Network's contractual agreements with content providers, is preserved.

14 **THE PIRACY OF DISH NETWORK PROGRAMMING**

15 30. Plaintiffs have developed and employ a robust Security System aimed at protecting
16 the copyrighted programming broadcast on DISH Network's satellite signals. This substantial and
17 costly security measure is necessary to prevent unauthorized access to DISH Network
18 Programming. The theft of Plaintiffs' encrypted signal and accompanying programming is
19 commonly referred to in the industry as "satellite piracy" (or "piracy"). Satellite piracy is a
20 problem that costs Plaintiffs tens of millions of dollars annually in the form of lost revenue, lost
21 subscribers, development and implementation of additional security features and electronic
22 counter-measures (or "ECMs") aimed at disabling pirate devices, and the investigation and
23 prosecution of the individuals responsible for the manufacturing, distribution and use of such
24 pirate devices.

25 31. Recently, satellite pirates and those working in concert developed a way to steal
26 DISH Network Programming using supposed "free-to-air" ("FTA") receivers. Older FTA
27 receivers were ostensibly used to receive unencrypted, freely available satellite transmissions such
28 as limited ethnic, religious, business, music, information, and advertising content. Free,

1 unencrypted satellite programming does not include the more sought-after programming offered in
2 subscription television packages, such as movie and sports channels, among others. Sonicview
3 receivers, however, are primarily designed, produced, marketed and used to descramble DISH
4 Network's encrypted satellite programming without authorization and without payment of
5 subscription fees. As explained below, Defendants sell and/or distribute various components,
6 software, firmware, hardware, codes, features and functionality which (a) are not necessary for the
7 reception and viewing of unencrypted FTA programming; and (b) are necessary for, and included
8 for the sole purpose of allowing the receivers to be used to intercept, decrypt and view DISH
9 Network's scrambled satellite signal and the copyrighted works broadcast thereon.

10 32. Pirating DISH Network Programming through the use of these Sonicview receivers
11 can be relatively inexpensive and effortless for consumers. This method of piracy is accomplished
12 by loading piracy related software and/or firmware (collectively "Pirate Software") that contains
13 proprietary keys and codes to Plaintiffs' Security System onto a Sonicview receiver, so as to
14 mimic a DISH Network Access Card. Pirate Software is made available on various internet
15 websites, including Defendants' websites www.sonicviewusa.com and www.ftalife.com, and, once
16 downloaded, is transferred to Sonicview receivers through various means including a connection
17 to a home computer or thumb drive. The process of loading Pirate Software is referred to as
18 "flashing" the receiver and can be completed in minutes.

19 33. A new form of satellite piracy has emerged known as Internet Key Sharing ("IKS")
20 or Control Word Sharing. IKS-enabled receivers, such as Sonicview's, contact a server (the "IKS
21 Server") over the Internet, which responds by providing a decrypted "control word" ("Control
22 Word"). The IKS Server has the ability to decrypt the Control Word because it is connected to a
23 legitimate subscribed or "hacked" DISH Network Access Card at the server location that decrypts
24 the Control Word. An IKS Server typically consists of multiple satellite receivers connected
25 together, each of which is responsible for descrambling specific channels.

26 34. Satellite receivers that support IKS, including Sonicview-brand receivers, pose a
27 unique threat to Plaintiffs for two primary reasons. First, unlike traditional satellite receivers
28 modified for piracy, which require hackers to generate a "fix" or "update" following an ECM, and

1 then require hackers or end-users to manually install it onto each satellite receiver affected by an
2 ECM, these IKS satellite receivers are designed to obtain all the information that they need to
3 descramble DISH Network Programming (including all "fixes" and "updates") directly from an
4 IKS Server via the Internet. These satellite receivers are thereby automatically immune to ECMs
5 and operate continuously to steal DISH Network Programming. Pirates often boast that these
6 receivers "never go down". Second, because these satellite receivers rely on the IKS Server, they
7 are able to descramble DISH Network Programming even after the completion of the transition to
8 new DISH Network Access Cards. For this reason, these satellite receivers effectively circumvent
9 the security enhancements found in newer generation DISH Network Access Cards.

10 35. Pirates, including Defendants, also sell and use devices known as "8PSK Turbo
11 Boards" or "DN Modules". These devices enable satellite receivers to receive satellite signals that
12 use a special form of modulation and forward error correction ("FEC") that is unique to the DISH
13 Network platform. Modulation is a method of varying wavelengths in a satellite signal to
14 communicate a message. FEC is a method of fixing corrupted portions of a satellite signal. These
15 8PSK modules contain what is known as "8PSK modulation" and "Turbo FEC". DISH Network's
16 High Definition ("HD") Programming is broadcasted using this unique combination of 8PSK
17 modulation and Turbo FEC. There are no FTA channels that broadcast programming using this
18 unique combination of modulation and FEC. There is no legitimate FTA purpose or use for these
19 8PSK modules. The only use for 8PSK modules is to receive DISH Network's HD Programming.

20 36. Pirates, including Defendants, also sell and use devices known as "Dongles" that
21 permit satellite receivers, including Sonicview receivers, to connect to the Internet using a
22 receiver's built in RS-232 port and thereby access an IKS Server for piracy purposes. Once a
23 "Dongle", such as the Sonicview I-Hub, is connected to a IKS-enabled satellite receiver, the user
24 simply downloads IKS Pirate Software from Defendants' websites, installs the Pirate Software,
25 and then enters the Internet address of the IKS Server. Once complete, the Sonicview receiver,
26 Sonicview I-Hub, 8PSK Turbo Board and Pirate Software work together to provide the customer
27 unlawful and unlimited access to DISH Network Programming without authorization from or
28 payment to DISH Network.

DEFENDANTS' WRONGFUL CONDUCT

1
2 37. Defendants Sonicview USA, Inc. Sonicviewra LLC, Sonicviewsa LLC, Roberto
3 Sanz, DontPay4TV, LLC, Duane Bernard and Courtney Bernard (collectively "Defendants") are
4 involved in and/or are responsible for designing, developing, manufacturing, importing,
5 distributing, trafficking-in, promoting and servicing piracy devices called Sonicview receivers
6 and/or components thereof (collectively "Sonicview Receivers"), and other circumvention devices
7 and/or components thereof including the Sonicview I-Hub and 8PSK Turbo Boards ("Pirate
8 Accessories"). These Sonicview Receivers and Pirate Accessories are (a) primarily designed or
9 produced for the purpose of circumventing Plaintiffs' Security System to gain access to DISH
10 Network Programming; (b) have only limited commercially significant purpose or use other than
11 to circumvent Plaintiffs' Security System to gain access to DISH Network Programming; or (c) are
12 marketed by Defendants and/or others acting in concert with Defendants for use in circumventing
13 Plaintiffs' Security System to gain access to DISH Network Programming.

Sonicview Receivers are Primarily Designed, Produced and Used for Piracy

14
15 38. Sonicview Receivers are specifically designed to accept and execute Pirate
16 Software that enables the receivers to circumvent DISH Network's Security System. Sonicview
17 Receivers include a variety of codes, components, features and functionality that have no
18 legitimate purpose or use for true FTA programming but which are used in Plaintiffs' Security
19 System. By way of example, some or all Sonicview Receivers contain embedded code that is
20 proprietary to DISH Network. Versions of this factory-installed software and firmware come pre-
21 installed on Sonicview Receivers and are also distributed at Sonicview's website,
22 www.sonicviewusa.com. There is no legitimate purpose for these proprietary codes to be included
23 in Sonicview Receivers and nor have Plaintiffs granted any of the Defendants authorization or
24 license for the use of these codes. The inclusion of these codes has no legitimate FTA purpose.

25 39. In addition to DISH Network's ROM and EEPROM codes, Sonicview receivers
26 also contain unauthorized copies of Security Keys used by DISH Network in their Security
27 System but which have no legitimate purpose or use for true FTA programming.
28

1 40. Sonicview Receivers include other features and functions that have no legitimate
2 purpose or use for true FTA programming and, instead, are included primarily to allow the
3 receivers to be used for DISH Network piracy. By way of example only, and without limitation,
4 these include: (a) a copy of NagraVision's patented IDEA Algorithm which is used as part of
5 Plaintiffs' efforts to secure its signal; and (b) hardware components unnecessary for FTA
6 programming such as microprocessors that include descrambling capabilities—a capability that
7 has no use for FTA programming in the United States. These items have no legitimate uses in
8 satellite television receivers intended for FTA use only.

9 41. Sonicview Receivers are primarily used for DISH Network piracy. Defendants are
10 aware that Sonicview Receivers are primarily used for DISH Network piracy. Defendants have
11 and/or are responsible for repairing, replacing or otherwise servicing Sonicview Receivers that
12 were returned to Sonicview with clear signs of piracy such as containing Pirate Software.

13 Sonicview I-Hubs are Primarily Designed, Produced and Used for Piracy

14 42. Defendants distribute IKS Dongles branded as "Sonicview I-Hubs". Sonicview I-
15 Hubs are primarily designed, produced and distributed for piracy. The only use of these devices is
16 satellite television piracy. Defendants distribute these devices to enable their customers to steal
17 unlimited amounts of DISH Network Programming through IKS piracy. The Sonicview I-Hubs
18 distributed by Defendants will not interface with a Sonicview Receiver without Pirate Software
19 distributed by Defendants at www.sonicviewusa.com or www.ftalife.com.

20 8PSK Turbo Boards are Primarily Designed, Produced and Used for Piracy

21 43. Defendants distribute "8PSK Turbo Boards" under the names Sub-Board, Q-Board,
22 and A-1 Board. 8PSK Turbo Boards are primarily designed, produced and distributed for piracy.
23 The only use for these devices is to receive DISH Network High Definition Programming.
24 Defendants distribute these devices to enable their customers to steal unlimited amounts of DISH
25 Network HD Programming. The 8PSK Boards distributed by Defendants will not interface with a
26 Sonicview Receiver without Pirate Software distributed by Defendants at www.sonicviewusa.com
27 or www.ftalife.com.

28

1 Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards are Promoted for Use in Piracy

2 44. Defendants and/or others acting in concert with them promote and advertise
3 Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards for use in the piracy of DISH Network
4 Programming. Defendants have engaged in and/or are responsible for one or more of the
5 following methods of promoting and advertising Sonicview Receivers, I-Hubs, and 8PSK Turbo
6 Boards for use in piracy: (a) using the logos of channels that are not available as free-to-air
7 channels and instead require a subscription; (b) giving out so-called "test boxes" to moderators,
8 administrators and/or other participants in piracy-related websites and online discussion forums in
9 exchange for favorable "write-ups or "reviews" which are posted on those websites and discuss the
10 ability of Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards to be used to steal DISH
11 Network Programming; (c) soliciting assistance of individuals involved in the online piracy
12 communities to promote Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards and their ability
13 to be used for piracy; (d) allowing Sonicview's trademarks and other intellectual property rights to
14 be used in various advertisements that promote Sonicview Receivers, I-Hubs, and 8PSK Turbo
15 Boards for their ability to pirate DISH Network Programming including through banner ads on
16 piracy-related websites; (e) posting hyperlinks on their websites that link to their Pirate Software
17 website, www.ftalife.com; and (f) posting hyperlinks on their Pirate Software website,
18 www.ftalife.com, linking to their other illicit websites that distribute Sonicview Receivers, I-Hubs,
19 and 8PSK Turbo Boards for use in piracy. Their website, www.ftalife.com, not only provides
20 consumers with illegal Pirate Software, but also offers instruction and information used to
21 descramble and steal DISH Network Programming.

22 Pirate Software are Primarily Designed, Produced, Used and Promoted for Piracy

23 45. Defendants and/or those acting on their behalf or in concert with them are involved
24 in and/or responsible for the design, development, financing and public release of Pirate Software
25 specifically tailored for use with Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards.

26 46. By causing or being responsible for the creation and release of Pirate Software,
27 Defendants ensure that Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards can be used for the
28

1 theft of DISH Network Programming thereby ensuring the continued sales of Sonicview
2 Receivers, I-Hubs, and 8PSK Turbo Boards.

3 47. Defendants have participated in and/or are responsible for the design, development,
4 financing and public release of numerous versions of Pirate Software. Different versions are
5 necessary for at least two purposes: (a) new versions tailored specifically for new models of
6 Sonicview Receivers, and I-Hubs and 8PSK Turbo Boards; and (b) new versions developed to
7 circumvent ECMs deployed by Plaintiffs to disable Sonicview Receivers being used for piracy.

8 48. Pirate Software is developed and distributed specifically for the purpose of
9 enabling Sonicview users to steal DISH Network Programming. The Pirate Software distributed
10 by Defendants and/or those acting on their behalf or in concert contains portions of software code
11 incorporated in Plaintiffs' Security System. These portions of code are proprietary to Plaintiffs'
12 Security System and include at least Plaintiffs' (a) EEPROM; (b) ROM; and (c) Security Keys.

13 49. There is no legitimate FTA purpose for the Pirate Software distributed by
14 Defendants. Defendants' Pirate Software has no commercially significant use or purpose other
15 than to circumvent Plaintiffs' Security System.

16 Defendants Intercept and Assist Others to Intercept DISH Network Programming

17 50. Defendants and/or others acting on their behalf or in concert with them intercept
18 DISH Network Programming. For example, Defendants "test" their 8PSK Turbo Boards prior to
19 distributing them. Because 8PSK Turbo Boards will not interface with a Sonicview Receiver
20 without the installation of Pirate Software distributed by Defendants, Defendants necessarily
21 install 8PSK Turbo Boards and Pirate Software onto Sonicview Receivers. Once the components
22 are assembled and installed, if the Sonicview Receiver can view DISH Network HD Programming
23 the "test" is considered successful.

24 51. Defendants' wrongful conduct described above is designed to and does assist others
25 to intercept DISH Network Programming.

26
27
28

CLAIMS FOR RELIEF

COUNT I AGAINST DEFENDANTS

(Circumventing a Technological Measure That Effectively Controls Access to a Work in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1))

52. Plaintiffs incorporate by reference paragraphs 1 through 51 as if set forth herein.

53. Plaintiffs' Security System is a technological measure that effectively controls access to DISH Network Programming.

54. Defendants were and are, and/or are responsible for, actively circumventing Plaintiffs' Security System to receive, without permission, authorization, or consent of Plaintiffs, DISH Network Programming in violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a)(1).

55. For example, Defendants claim to "test" 8PSK Turbo Boards prior to distribution. Thus, Defendants necessarily install 8PSK Boards and Pirate Software into Sonicview Receivers for "testing" purposes. If the Sonicview Receiver then successfully circumvents DISH Network's Security System and can view DISH Network HD Programming, then the test is considered successful.

56. Defendants violated Section 1201(a)(1) of the DMCA willfully and for purposes of commercial advantage or private financial gain.

57. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendants will continue to violate Section 1201(a)(1) of the DMCA.

COUNT II AGAINST DEFENDANTS

(Manufacture, Import, Offer to the Public, Provide, or Otherwise Traffic in Technologies, Products, Services, Devices, Components, or Parts Thereof in Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1))

58. Plaintiffs incorporate by reference paragraphs 1 through 51 as if set forth herein.

59. Defendants were and are actively engaged in the in the business of manufacturing, importing, offering to the public, providing, or otherwise trafficking in unlawful technologies,

1 products, services, devices, components, or parts thereof in violation of the DMCA, 17 U.S.C. §§
2 1201(a)(2) and 1201(b)(1).

3 60. Sonicview Receivers, I-Hubs, 8PSK Turbo Boards, and Pirate Software provided
4 by Defendants are: (1) designed or produced for the purpose of circumventing Plaintiffs' Security
5 System—a technological measure that effectively controls access to, copying and distribution of,
6 copyrighted works; (2) made available by Defendants despite having no commercially significant
7 purpose or use other than to circumvent Plaintiffs' Security System; and/or (3) marketed by
8 Defendants and/or through others acting in concert with knowledge that they are used to
9 circumvent Plaintiffs' Security System and for use in circumventing Plaintiffs' Security System.

10 61. Defendants were and are manufacturing, importing, offering to the public,
11 providing, or otherwise trafficking in pirate technology including Sonicview Receivers, I-Hubs,
12 8PSK Turbo Boards, and Pirate Software with knowledge that these technologies, products,
13 devices, components, or parts thereof are used to circumvent Plaintiffs' Security System—a
14 technological measure that effectively controls access to, copying and distribution of, copyrighted
15 works.

16 62. Defendants' actions that constitute violations of the DMCA were performed
17 without permission, authorization, or consent of Plaintiffs or any owner of copyrighted
18 programming broadcast on the DISH Network platform.

19 63. Defendants violated Sections 1201(a)(2) and 1201(b)(1) of the DMCA willfully
20 and for purposes of commercial advantage or private financial gain.

21 64. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an
22 amount to be proven at trial. Unless permanently restrained and enjoined by the Court,
23 Defendants will continue to violate Sections 1201(a)(2) and 1201(b)(1) of the DMCA.

24 **COUNT III AGAINST DEFENDANTS**

25 **(Facilitating the Unauthorized Decryption and Reception of Satellite Signals in Violation of**
26 **the Communications Act, 47 U.S.C. § 605(a))**

27 65. Plaintiffs incorporate by reference paragraphs 1 through 51 as if set forth herein.
28

1 66. Defendants were intercepting and/or are assisting others, including those that
2 purchased Sonicview Receivers, I-Hubs, and 8PSK Turbo Boards, and downloaded corresponding
3 Pirate Software from Defendants' websites, to intercept and receive DISH Network Programming
4 without authorization and for their own benefit in violation of the Communications Act, 47 U.S.C.
5 § 605(a).

6 67. Defendants were and are assisting, directly or indirectly, with the design,
7 manufacture, development, assembly, modification, solicitation, and/or distribution of pirate
8 technology including Sonicview Receivers, I-Hubs, 8PSK Turbo Boards, and Pirate Software with
9 knowledge, or having reason to know, that such devices, technologies, and services are used
10 primarily to assist in the unauthorized interception and decryption of direct-to-home satellite
11 services in violation of the Communications Act, 47 U.S.C. § 605(a).

12 68. Defendants violated 47 U.S.C. § 605(a) of the Communications Act willfully and
13 for the purpose of direct or indirect commercial advantage or private financial gain.

14 69. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an
15 amount to be proven at trial. Unless permanently restrained and enjoined by the Court,
16 Defendants will continue to violate the alleged provisions of the Communications Act.

17 **COUNT IV AGAINST DEFENDANTS**

18 **(Manufacture and Sale of Signal Theft Devices and Technology in Violation of the**
19 **Communications Act, 47 U.S.C. § 605(e)(4))**

20 70. Plaintiffs incorporate by reference paragraphs 1 through 51 as if set forth herein.

21 71. Defendants were and are engaged in the business of designing, manufacturing,
22 developing, assembling, modifying, importing, exporting, selling, or otherwise distributing pirate
23 technology including Sonicview Receivers, I-Hubs, 8PSK Turbo Boards, and Pirate Software to
24 facilitate the illegal use and reception of DISH Network Programming in violation of the
25 Communications Act, 47 U.S.C. § 605(e)(4).

26 72. Defendants were and are assisting, directly or indirectly, with the design,
27 manufacture, development, assembly, modification, solicitation, and/or distribution of pirate
28 technology including Sonicview Receivers, I-Hubs, 8PSK Turbo Boards, and Pirate Software with

1 knowledge, or having reason to know, that such devices and technology were and are used
2 primarily to assist in the unauthorized interception and decryption of direct-to-home satellite
3 services in violation of the Communications Act, 47 U.S.C. § 605(e)(4).

4 73. Defendants violated Section 605(e)(4) of the Communications Act willfully and for
5 the purpose of direct or indirect commercial advantage or private financial gain.

6 74. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an
7 amount to be proven at trial. Unless permanently restrained and enjoined by the Court,
8 Defendants will continue to violate the alleged provisions of the Communications Act.

9 **COUNT V AGAINST DEFENDANTS**

10 **(Unauthorized Interception of Electronic Communications in Violation of the Electronic**
11 **Communications Privacy Act, 18 U.S.C. § 2511(1)(a))**

12 75. Plaintiffs incorporate by reference paragraphs 1 through 51 as if set forth herein.

13 76. Defendants were and are, and/or are responsible for intentionally intercepting DISH
14 Network's encrypted satellite transmissions in violation of the Electronic Communications Privacy
15 Act ("Wiretap Act"), 18 U.S.C. § 2511(1)(a), by facilitating the use of pirate technology including
16 Sonicview Receivers, I-Hubs, 8PSK Turbo Boards, and Pirate Software.

17 77. Defendants knew that the interception of DISH Network's encrypted satellite
18 signals was and is illegal and prohibited.

19 78. Defendants violated section 2511(1)(a) of the Wiretap Act for a tortious or illegal
20 purpose, or for purposes of direct or indirect commercial advantage or private financial gain.

21 79. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an
22 amount to be proven at trial. Unless permanently restrained and enjoined by the Court,
23 Defendants will continue to violate the alleged provisions of the Wiretap Act.

24 **PRAYER FOR RELIEF**

25 WHEREFORE, Plaintiffs seek judgment against Defendants as follows:

- 26 A. For a grant of permanent injunctive relief restraining and enjoining Defendants, and
27 their employees, agents, representatives, attorneys, and all persons acting or
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

claiming to act on their behalf or under their direction or authority, and all persons acting in concert or in participation with them, from:

- 1) offering to the public, providing, or otherwise trafficking in any FTA receivers, Pirate Software, or any other device, component, or technology, or part thereof, through any means including Internet websites, that:
 - a) is primarily designed or produced for the purpose of circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform;
 - b) have only a limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform;
 - c) is knowingly marketed by Defendants and/or others acting in concert with Defendants for use in circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform; and
- 2) assembling, modifying, selling, and/or distributing any FTA Receivers or Pirate Software knowing or having reason to know that such device or software is primarily of assistance in the unauthorized decryption of direct-to-home satellite services through any means including Internet websites;

- 1 3) receiving Plaintiffs' electronic communications without Plaintiffs'
2 authorization through any means; and
3 4) assisting others in receiving (including assistance offered by providing
4 hypertext links or banner advertising) Plaintiffs' electronic communications
5 without Plaintiffs' authorization through any means including Internet
6 websites.

7 B. For an Order impounding all electronic copies of Pirate Software, FTA Receivers,
8 or other circumvention or signal theft technology, components, or devices in the
9 custody or control of Defendants or related entities that the Court has reasonable
10 cause to believe were involved in a violation of the Digital Millennium Copyright
11 Act, 17 U.S.C. § 1201 *et seq.*

12 C. For an Order directing Defendants to preserve and maintain all records, in any form
13 (including electronic form), that evidence, refer, or relate to: FTA Receivers, Pirate
14 Software, communications or correspondence with suppliers of software, hardware,
15 or other equipment or know-how concerning satellite television piracy, including
16 any dealer, distributor, or manufacturer of FTA Receivers.

17 D. Award Plaintiffs the greater of its actual damages together with any profits made by
18 Defendants that are attributable to the violations alleged herein, or statutory
19 damages in the amount of up to \$10,000 for each violation of 47 U.S.C. § 605(a),
20 pursuant to 47 U.S.C. § 605(e)(3)(C)(i).

21 E. Award Plaintiffs discretionary damages in the amount of up to \$100,000 for each
22 violation of 47 U.S.C. § 605(a), pursuant to 47 U.S.C. § 605(e)(3)(C)(ii).

23 F. Award Plaintiffs the greater of its actual damages together with any profits made by
24 Defendants that are attributable to the violations alleged herein, or statutory
25 damages in the amount of up to \$100,000 for each violation of 47 U.S.C. §
26 605(e)(4), pursuant to 47 U.S.C. § 605(e)(3)(C)(i).

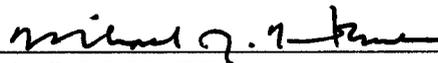
27 G. Award Plaintiffs the greater of its actual damages together with any profits made by
28 Defendants that are attributable to the violations alleged herein, or statutory

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- damages in the amount of up to \$2,500 for each violation of 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1), pursuant to 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A).
- H. Award Plaintiffs the greater of its actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of \$100 per day for each violation of 18 U.S.C. § 2511(1) or \$10,000, pursuant to 18 U.S.C. § 2520(c)(2).
- I. Award Plaintiffs punitive damages afforded by law pursuant to 18 U.S.C. § 2520(b)(2), and in equity for unjust enrichment.
- J. For an award of Plaintiffs' costs, reasonable attorneys' fees, and investigative fees.
- K. For pre- and post-judgment interest on all profits and damages granted by this Court in accordance with the law.
- L. For such other and further relief as the Court deems just and proper.

Dated: July 17, 2009

ALLEN MATKINS LECK GAMBLE
MALLORY & NATSIS LLP

By: 
MARK J. HATTAM
MICHAEL J. HOLMES

HAGAN NOLL & BOYLE LLC
CHAD M. HAGAN (*pro hac vice* pending)
DAVID M. NOLL (*pro hac vice* pending)
CLAYTON D. CRAIGHEAD (*pro hac vice* pending)
Attorneys for Plaintiffs

CIVIL COVER SHEET

JS 44 (Rev. 12/07)

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

FILED
JUL 17 2009
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
San Diego, CA

I. (a) PLAINTIFFS

DISH Network LLC, et al.

DEFENDANTS

Sonievview USA, Inc., et al.

(b) County of Residence of First Listed Plaintiff Arapahoe County, CO
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED.

Attorneys (If Known)

(c) Attorney's (Firm Name, Address, and Telephone Number)
ALLEN MATKINS LECK GAMBLE MALLORY & NATSIS LLP, 501 West Broadway, 15th Floor, San Diego, CA 92101, (619) 233-1155

09 CV 1553 H NLS

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
2 U.S. Government Defendant
3 Federal Question (U.S. Government Not a Party)
4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- Citizen of This State
Citizen of Another State
Citizen or Subject of a Foreign Country
Incorporated or Principal Place of Business In This State
Incorporated and Principal Place of Business In Another State
Foreign Nation

IV. NATURE OF SUIT (Place an "X" in One Box Only)

- 110 Insurance
120 Marine
130 Miller Act
140 Negotiable Instrument
150 Recovery of Overpayment & Enforcement of Judgment
151 Medicare Act
152 Recovery of Defaulted Student Loans (Excl. Veterans)
153 Recovery of Overpayment of Veteran's Benefits
160 Stockholders' Suits
190 Other Contract
195 Contract Product Liability
196 Franchise
PERSONAL INJURY
310 Airplane
315 Airplane Product Liability
320 Assault, Libel & Slander
330 Federal Employers' Liability
340 Marine
345 Marine Product Liability
350 Motor Vehicle
355 Motor Vehicle Product Liability
360 Other Personal Injury
PERSONAL INJURY
362 Personal Injury - Med. Malpractice
365 Personal Injury - Product Liability
368 Asbestos Personal Injury Product Liability
PERSONAL PROPERTY
370 Other Fraud
371 Truth in Lending
380 Other Personal Property Damage
385 Property Damage Product Liability
610 Agriculture
620 Other Food & Drug
625 Drug Related Seizure of Property 21 USC 881
630 Liquor Laws
640 R.R. & Truck
650 Airline Regs.
660 Occupational Safety/Health
690 Other
422 Appeal 28 USC 158
423 Withdrawal 28 USC 157
400 State Reapportionment
410 Antitrust
430 Banks and Banking
450 Commerce
460 Deportation
470 Racketeer Influenced and Corrupt Organizations
480 Consumer Credit
490 Cable/Sat TV
810 Selective Service
850 Securities/Commodities/Exchange
875 Customer Challenge 12 USC 3410
890 Other Statutory Actions
891 Agricultural Acts
892 Economic Stabilization Act
893 Environmental Matters
894 Energy Allocation Act
895 Freedom of Information Act
900 Appeal of Fee Determination (Under Equal Access to Justice)
950 Constitutionality of State Statutes

V. ORIGIN

- 1 Original Proceeding
2 Removed from State Court
3 Remanded from Appellate Court
4 Reinstated or Reopened
5 Transferred from another district (specify)
6 Multidistrict Litigation
7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing. (Do not cite jurisdictional statutes unless obligatory.)
47 U.S.C. Section 1201, et al., 17 U.S.C. Section 605, et al.
28 USC 1331
Brief description of cause:
Defendants distribute satellite television piracy devices and software.

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23
DEMAND \$
CHECK YES only if demanded in complaint:
JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE: 07/17/09
SIGNATURE OF ATTORNEY OF RECORD: [Signature]

FOR OFFICE USE ONLY
RECEIPT # 3098 AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44**Authority For Civil Cover Sheet**

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerks in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553
Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

Court Name: USDC California Southern
Division: 3
Receipt Number: CAS003098
Cashier ID: sramirez
Transaction Date: 07/17/2009
Payer Name: CALEXPRESS

CIVIL FILING FEE
For: DISH NETWORK V. SONICVIEW
Case/Party: D-CAS-3-09-CV-001553-001
Amount: \$350.00

CHECK
Check/Money Order Num: 49195
Amt Tendered: \$350.00

Total Due: \$350.00
Total Tendered: \$350.00
Change Amt: \$0.00

There will be a fee of \$45.00
charged for any returned check.