

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

J. BRUCE ALVERSON, ESQ.  
Nevada Bar No. 1339  
KARIE N. WILSON, ESQ.  
Nevada Bar No. 7957  
**ALVERSON TAYLOR**  
**MORTENSEN & SANDERS**  
7401 W. Charleston Boulevard  
Las Vegas, NV 89117  
702-384-7000 Phone  
702-385-7000 Fax  
Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

DISH NETWORK LLC, a Colorado Limited  
Liability Company, ECHOSTAR  
TECHNOLOGIES LLC, a Texas Limited Liability  
Company, and NAGRASTAR LLC, a Colorado  
Limited Liability Company,

Plaintiffs

v.

MICHAEL CHO, an individual, JASON CHO,  
an individual, MAMERTINE, INC., an Oklahoma  
Corporation, each and together dba NFUSION,

Defendants

CASE NO:

**PLAINTIFFS' ORIGINAL  
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);

Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C. and NagraStar LLC

(collectively "DISH Network") bring this suit against defendants for violation of the Digital Millennium Copyright Act, the Communications Act and related statutes.

### **INTRODUCTION & NATURE OF THE ACTION**

1. DISH Network provides more than 14 million customers with high quality satellite television programming. DISH Network's customers have access to hundreds of video and audio channels, the most high definition (HD) channels, the most international channels, state-of-the-art interactive TV applications, and award-winning HD and digital video recorder technology. DISH Network provides its service to customers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price) to DISH Network.

2. Defendants Michael Cho and Jason Cho are satellite pirates who distribute devices that enable consumers to illegally intercept and decrypt DISH Network's pay-television programming without authorization and without payment of a subscription fee to DISH Network. Michael Cho and Jason Cho perform their illegal acts individually and under the name of their business Mamertine, Inc. d/b/a NFUSION and NFUSION, Inc.

3. Defendants' conduct violates a variety of federal statutes, including the Digital Millennium Copyright Act and the Communications Act.

4. DISH Network bring this suit seeking civil impoundment of defendants' devices and software under the impoundment provisions of the Digital Millennium Copyright Act, for a permanent injunction barring defendants from trafficking in such devices, for damages and for such other relief as plaintiffs prove themselves entitled.

### **JURISDICTION AND VENUE**

5. This court has original federal question subject matter jurisdiction under 28 U.S.C. §§ 1331 because the claims are based upon the Digital Millennium Copyright Act, 17

1 U.S.C. § 1201 et seq., the Communications Act of 1934, as amended, 47 U.S.C. § 605 et seq.,  
 2 and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 et seq.

3 6. Personal jurisdiction and venue are proper in this court pursuant to 28 U.S.C. §§  
 4 1391(b)(1) because at least one defendant resides within this judicial district, § 1391(b)(2)  
 5 because a substantial part of the events giving rise to this action occurred in this judicial district,  
 6 § 1391(b)(3) because defendants may be found in this judicial district and are subject to in  
 7 personam jurisdiction, and §1400(a) because this case is related to an Act of Congress related to  
 8 copyrights and the defendants and/or their agents may be found in this district.

### 9 PARTIES<sup>1</sup>

10 7. Plaintiff DISH Network L.L.C. is a Colorado limited liability company with its  
 11 principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112,  
 12 Arapahoe County. Plaintiff DISH Network L.L.C.'s sole member is DISH DBS Corporation, a  
 13 Colorado Corporation, which in turn is an indirect wholly owned subsidiary of DISH Network  
 14 Corporation, a Nevada Corporation. DISH Network Corporation is publicly owned and traded  
 15 on the NASDAQ national market under the symbol "DISH."

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

21 ...

---

23 1 DISH Network's allegations related to the wrongful conduct of defendants are based upon the  
 24 investigation DISH Network has completed to date, upon information and 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.

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

10. Upon information and belief, defendant Michael Cho is co-owner of Mamertine, Inc. and does business under the assumed name NFusion. Upon information and belief, Michael Cho resides and may be served at 2880 BICENTENNIAL PKWY STE 100, HENDERSON NV 89044-4484.

11. Upon information and belief, defendant Jason Cho is co-owner of Mamertine, Inc. and does business under the assumed name NFusion. Jason Cho resides and may be served at 2880 BICENTENNIAL PKWY STE 100, HENDERSON NV 89044-4484. Alternatively, Jason Cho may be served at 6025 Southernness Dr., El Dorado Hills, Ca. 95762.

12. Defendant Mamertine, Inc. is an Oklahoma corporation with its principal place of business at 302 South Peoria, Tulsa, Oklahoma, and has done business in this district through its corporate officers Michael Cho and Jason Cho. Mamertine, Inc. may be served by service upon its officers Michael Cho or Jason Cho.

13. Each defendant individually, and together, does business as NFusion and NFusion, Inc. (including using various alternate spellings such as "nfusion," collectively "NFusion"). NFusion is an assumed name and d/b/a of Michael Cho, Jason Cho, and Mamertine, Inc. NFusion is also the brand name defendants use for their satellite receivers.

...

15. Any judgment pursuant to DISH Network's request for relief should be rendered joint and several against defendants Michael Cho, Jason Cho, and Mamertine, Inc.

16. DISH Network provides more than 14 million customers with high quality satellite television programming. DISH Network's customers have access to hundreds of video and audio channels, the most high definition (HD) channels, the most international channels, state-of-the-art interactive TV applications, and award-winning HD and digital video recorder (DVR) technology. DISH Network provides its service to customers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price) to DISH Network.

18. Because DISH Network generates revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain distribution rights for programming is dependent upon preventing unauthorized reception of DISH Network Programming, DISH Network's video channels (except for certain promotional

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 channels) are digitally secured and encrypted.

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

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

16 21. A consumer wishing to subscribe to and receive DISH Network Programming  
17 must first have the necessary equipment which consists primarily of: a satellite dish; an  
18 integrated receiver/decoder; and a credit card-sized DISH Network Access Card that is loaded  
19 into the receiver through a slot on the face of the receiver. On some newer models, the Access  
20 Card is integrated directly into the satellite receiver itself and is not removable.

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

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1           23.     DISH Network provides its Access Cards to customers for use with the receivers  
2     for the purpose of enabling authorized access to DISH Network Programming. Without a  
3     subscription, DISH Network will not provide a consumer an Access Card or authorize access to  
4     encrypted DISH Network Programming. Subscribers are not authorized to modify or tamper  
5     with the Access Card, which are clearly marked as property of DISH Network and must be  
6     returned upon request.

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

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

18           26.     The ROM code segment provides detailed instructions and commands to DISH  
19    Network Access Cards and receivers in the normal operation of plaintiffs' Security System.  
20    Access to the proprietary information stored in the ROM code is necessary to unlock the safe  
21    containing the secrets to plaintiffs' Security System.

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



ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 including, but not limited to “transmission” keys and “pairing” keys (collectively known as  
2 “Security Keys”). The Security Keys are used, inter alia, to encrypt and decrypt the  
3 communications between the DISH Network Access Card and the receiver.

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

8 29. DISH Network’s Security System effectively controls access to the copyrighted  
9 materials that comprise DISH Network Programming. In addition, the Security System ensures  
10 that the protection afforded to such copyrighted works, such as limitations on the dissemination  
11 and use in accordance with DISH Network’s contractual agreements with content providers, is  
12 preserved. This substantial and costly security measure is necessary to prevent unauthorized  
13 access to DISH Network Programming. The theft of DISH Network’s encrypted signal and  
14 accompanying programming is commonly referred to in the industry as “satellite piracy” (or  
15 “piracy”). Satellite piracy is a problem that costs DISH Network tens of millions of dollars  
16 annually in the form of lost revenue, lost subscribers, development and implementation of  
17 additional security features and electronic counter-measures (or “ECMs”) aimed at disabling  
18 pirate devices, and the investigation and prosecution of the individuals responsible for the  
19 manufacturing, distribution and use of such pirate devices.

20 **Defendants’ Devices Are Designed To Circumvent Plaintiffs’ Security System.**

21 30. Defendants are involved in and/or are responsible for designing, developing,  
22 manufacturing, importing, distributing, trafficking-in, promoting and servicing piracy devices  
23 called NFusion Receivers and/or components thereof (collectively “NFusion Receivers”), and  
24 other circumvention devices and/or components thereof including the NFusion 8PSK Turbo



ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 Board and NFusion pirate software. These devices and technology are (a) primarily designed or  
2 produced for the purpose of circumventing DISH Network's Security System to gain access to  
3 DISH Network Programming; (b) have only limited commercially significant purpose or use  
4 other than to circumvent DISH Network's Security System to gain access to DISH Network  
5 Programming; or (c) are marketed by defendants and/or others acting in concert with defendants  
6 for use in circumventing DISH Network's Security System to gain access to DISH Network  
7 Programming.

8 31. Defendants' NFusion Receivers and pirate software are designed to and utilize a  
9 new form of satellite piracy known as Internet Key Sharing ("IKS") (and sometimes referred to  
10 as Control Word Sharing). IKS involves connecting an NFusion Receiver to the Internet to  
11 obtain keys that are necessary to decrypt DISH Network Programming. Defendants and their  
12 pirate end-users use a satellite dish to intercept DISH Network's encrypted satellite transmission  
13 that is intended for legitimate and authorized DISH Network subscribers.

14 32. Once defendants' NFusion Receiver intercepts DISH Network's encrypted  
15 satellite transmission, it locates a special part of the satellite transmission known as the encrypted  
16 Entitlement Control Message and sends that encrypted Entitlement Control Message over the  
17 Internet to the computer server (the "NFusion IKS Server"). The NFusion IKS Server, through  
18 its connection to a either legitimate and subscribed or a "hacked" DISH Network Access Card,  
19 decrypts the Control Word and sends it back to the end-user's NFusion Receiver. Once returned  
20 to the NFusion Receiver by the NFusion IKS Server, the decrypted Control Word acts like a key  
21 that unscrambles the otherwise-scrambled and encrypted DISH Network Programming, allowing  
22 each end-user to steal DISH Network Programming.

23 33. NFusion Receivers are designed for and do engage in IKS piracy and therefore  
24 pose a unique threat to DISH Network for two primary reasons. First, unlike traditional satellite

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

12 34. NFusion Receivers are specifically designed to accept and execute pirate software  
13 that enables the receivers to circumvent DISH Network’s Security System. NFusion Receivers  
14 include a variety of components, features and functionality that have no legitimate purpose or  
15 use for true FTA programming but which are useful and/or necessary to circumvent DISH  
16 Network’s Security System and steal DISH Network Programming.

17 35. Defendants also sell and use devices known as “8PSK Turbo Boards” or “DN  
18 Modules.” These devices enable satellite receivers to receive satellite signals that use a special  
19 form of modulation and forward error correction that is unique to the DISH Network platform.  
20 Modulation is a method of varying wavelengths in a satellite signal to communicate a message.  
21 Forward error correction (“FEC”) is a method of fixing corrupted portions of a satellite signal.  
22 These 8PSK Turbo Boards contain what is known as “8PSK modulation” and “Turbo FEC.”  
23 DISH Network’s High Definition (“HD”) Programming is broadcasted using this unique  
24 combination of 8PSK modulation and Turbo FEC. There are no FTA channels that broadcast

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 programming using this unique combination of modulation and FEC and therefore no legitimate  
2 FTA purpose or use for NFusion 8PSK Turbo Boards. The only use for NFusion 8PSK Turbo  
3 Boards is to enable NFusion Receivers to steal DISH Network's HD Programming.

4 36. Defendants and their pirate end-users connect NFusion Receivers directly to the  
5 Internet using a built-in Ethernet port that provides access to the NFusion IKS Server for piracy  
6 purposes. Once connected to an IKS-enabled satellite receiver, the user simply downloads the  
7 defendants' pirate software, installs the pirate software onto their NFusion Receiver, and enters  
8 the Internet address of the NFusion IKS Server. Alternatively, the consumer buys an NFusion  
9 Receiver with pirate software pre-installed. Once completed, the NFusion Receiver allows the  
10 end-user unlawful and unlimited access to DISH Network Programming without authorization  
11 from or payment to DISH Network.

12 37. NFusion Receivers are primarily used for DISH Network piracy. Defendants are  
13 aware that NFusion Receivers are primarily used for DISH Network piracy. Defendants have  
14 and/or are responsible for repairing, replacing or otherwise servicing NFusion Receivers that  
15 were returned to NFusion with clear signs of piracy such as containing pirate software and/or  
16 8PSK Turbo Boards.

17 **Defendants' Pirate Software Is Designed To Circumvent DISH Network's Security System.**

18 38. Defendants and/or those acting on their behalf or in concert with them are  
19 involved in and/or responsible for the design, development, financing and public release of pirate  
20 software specifically designed to use with NFusion Receivers and 8PSK Turbo Boards.

21 39. By causing or being responsible for the creation and release of pirate software,  
22 defendants ensure that NFusion Receivers and 8PSK Turbo Boards can be used to steal DISH  
23 Network Programming thereby ensuring the continued sales of NFusion Receivers and 8PSK  
24 Turbo Boards.

ALVERSON, TAYLOR, MORTENSEN & SANDERS

LAWYERS

7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1           40. Defendants have participated in and/or are responsible for the design,  
2 development, financing and public release of numerous versions of pirate software. Different  
3 versions are necessary for at least two purposes: (a) new versions tailored specifically for new  
4 models of NFusion Receivers and 8PSK Turbo Boards; and (b) new versions developed to  
5 circumvent ECMs deployed by DISH Network to disable NFusion Receivers from being used for  
6 piracy.

7           41. Defendants' pirate software is (a) primarily designed or produced for the purpose  
8 of circumventing DISH Network's Security System to gain access to DISH Network  
9 Programming; (b) has only limited commercially significant purpose or use other than to  
10 circumvent DISH Network's Security System to gain access to DISH Network Programming; or  
11 (c) is marketed by defendants and/or others acting in concert with defendants for use in  
12 circumventing DISH Network's Security System to gain access to DISH Network Programming.

13           42. Defendants have participated in and/or are responsible for distribution of  
14 numerous versions of pirate software. There is no legitimate use for the pirate software  
15 distributed by defendants. Defendants' pirate software has no commercially significant use or  
16 purpose. The only use for defendants' pirate software is to circumvent DISH Network's Security  
17 System.

18           43. Defendants and those acting on their behalf or in concert with them circumvent  
19 DISH Network's Security System, intercept satellite signals and copyrighted programming  
20 distributed by DISH Network, view such programming without authorization, and redistribute  
21 some of such programming to others without authorization.

22 ...

23 ...

24 ...

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 **Defendants' Devices and Software Are Advertised As Circumvention Devices.**

2 44. Defendants and/or others acting in concert with them promote and advertise  
3 NFusion Receivers, 8PSK Turbo Boards and pirate software for use in the piracy of DISH  
4 Network Programming.

5 45. Defendants have engaged in and/or are responsible for one or more of the  
6 following methods of promoting and advertising NFusion Receivers and 8PSK Turbo Boards for  
7 use in piracy: (a) using the logos of channels that are not available as free-to-air channels and  
8 instead require a subscription; (b) giving out so-called "test boxes" to moderators, administrators  
9 and/or other participants in piracy-related websites and online discussion forums in exchange for  
10 favorable "write-ups or "reviews" which are posted on those websites and discuss the ability of  
11 NFusion Receivers and 8PSK Turbo Boards to be used to steal DISH Network Programming; (c)  
12 soliciting assistance of individuals involved in the online piracy communities to promote  
13 NFusion Receivers and 8PSK Turbo Boards and their ability to be used for piracy; and (d)  
14 allowing NFusion's trademarks and other intellectual property rights to be used in various  
15 advertisements that promote NFusion Receivers and 8PSK Turbo Boards for their ability to  
16 pirate DISH Network Programming including through banner ads on piracy-related websites.

17 **Defendants' Themselves Circumvent DISH Network's Security System.**

18 46. Defendants and those acting on their behalf or in concert with them circumvent  
19 DISH Network's Security System in two ways. First, defendants are involved with and operate  
20 the NFusion IKS Server. The NFusion IKS Server's role is to circumvent DISH Network's  
21 Security System and transmit control words to connected NFusion Receivers in violation of the  
22 statutes enumerated herein. Second, defendants' use, demonstration, testing and design of their  
23 devices and pirate software involves the actual circumvention of DISH Network's Security  
24 System and interception of DISH Network Programming. For example, Defendant Michael Cho

1 used NFusion Receivers and pirate software to receive unlimited DISH Network Programming in  
2 his home.

### 3 CLAIMS FOR RELIEF

#### 4 COUNT 1

#### 5 **(Circumventing a Technological Measure That Effectively Controls Access to a Work in** 6 **Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1))**

7 47. DISH Network incorporates the preceding paragraphs as if set forth herein.

8 48. DISH Network's Security System is a technological measure that effectively  
9 controls access to DISH Network Programming.

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

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

16 51. Defendants' misconduct has and will continue to cause damage to DISH Network  
17 in an amount to be proven at trial. Unless permanently restrained and enjoined by the court,  
18 defendants will continue to violate Section 1201(a)(1) of the DMCA.

#### 19 COUNT 2

#### 20 **(Manufacture, Import, Offer to the Public, Provide, or Otherwise Traffic in Technologies,** 21 **Products, Services, Devices, Components, or Parts Thereof in Violation of the Digital** 22 **Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1))**

23 52. DISH Network incorporates the preceding paragraphs as if set forth herein.

24 ...

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

53. Defendants were and are actively engaged in the business of distributing unlawful technologies, products, services, components, or parts thereof in violation of the DMCA, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1).

54. Defendants' devices and pirate software are: (1) designed or produced for the purpose of circumventing DISH Network's Security System—a technological measure that effectively controls access to, copying and distribution of, copyrighted works; (2) made available by defendants despite having no commercially significant purpose or use other than to circumvent DISH Network's Security System; and/or (3) marketed by defendants and/or through others acting in concert with knowledge that they are used to circumvent DISH Network's Security System and for use in circumventing DISH Network's Security System.

55. Defendants were and are distributing pirate devices and software with knowledge that these technologies, products, services, components, or parts thereof are used to circumvent DISH Network's Security System.

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

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

58. Defendants' misconduct has and will continue to cause damage to DISH Network in an amount to be proven at trial. Unless permanently restrained and enjoined by the court, defendants will continue to violate Sections 1201(a)(2) and 1201(b)(1) of the DMCA.

...

...

...



ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

**COUNT 3**

**(Facilitating the Unauthorized Decryption and Reception of Satellite Signals**

**in Violation of the Communications Act, 47 U.S.C. § 605(a))**

59. DISH Network incorporates the preceding paragraphs as if set forth herein.

60. Defendants were intercepting and/or are assisting others to intercept and receive DISH Network Programming without authorization and for their own benefit in violation of the Communications Act, 47 U.S.C. § 605(a).

61. Defendants were and are assisting, directly or indirectly, with the design, manufacture, development, assembly, modification, solicitation, and/or distribution of pirate software with knowledge, or having reason to know, that such technologies and services are used primarily to assist in the unauthorized interception and decryption of direct-to-home satellite services in violation of the Communications Act, 47 U.S.C. § 605(a).

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

63. Defendants' misconduct has and will continue to cause damage to DISH Network in an amount to be proven at trial. Unless permanently restrained and enjoined by the court, defendants will continue to violate the alleged provisions of the Communications Act.

**COUNT 4**

**(Manufacture and Sale of Signal Theft Devices and Technology in Violation of the**

**Communications Act, 47 U.S.C. § 605(e)(4))**

64. DISH Network incorporates the preceding paragraphs as if set forth herein.

65. Defendants were and are engaged in the business of designing, manufacturing, developing, assembling, modifying, importing, exporting, selling, or otherwise distributing pirate devices and software to facilitate the illegal use and reception of DISH Network Programming in

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 violation of the Communications Act, 47 U.S.C. § 605(e)(4).

2 66. Defendants were and are assisting, directly or indirectly, with the design,  
3 manufacture, development, assembly, modification, solicitation, and/or distribution of pirate  
4 devices and software with knowledge, or having reason to know, that such devices and  
5 technology were and are used primarily to assist in the unauthorized interception and decryption  
6 of direct-to-home satellite services in violation of the Communications Act, 47 U.S.C. §  
7 605(e)(4).

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

10 68. Defendants' misconduct has and will continue to cause damage to DISH Network  
11 in an amount to be proven at trial. Unless permanently restrained and enjoined by the court,  
12 defendants will continue to violate the alleged provisions of the Communications Act.

### 13 COUNT 5

#### 14 **(Unauthorized Interception of Electronic Communications in Violation of the Electronic** 15 **Communications Privacy Act, 18 U.S.C. § 2511(1)(a))**

16 69. DISH Network incorporates the preceding paragraphs as if set forth herein.

17 70. Defendants were and are intentionally intercepting DISH Network's encrypted  
18 satellite transmissions in violation of the Electronic Communications Privacy Act ("Wiretap  
19 Act"), 18 U.S.C. § 2511(1)(a), by facilitating the use of pirate software.

20 71. Defendants knew that the interception of DISH Network's encrypted satellite  
21 signals was and is illegal and prohibited.

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

24 ...

ALVERSON, TAYLOR, MORTENSEN & SANDERS  
LAWYERS  
7401 WEST CHARLESTON BOULEVARD  
LAS VEGAS, NEVADA 89117-1401  
(702) 384-7000

1 distributor, or manufacturer of FTA Receivers.

2 D. Award DISH Network the greater of its actual damages together with any profits  
3 made by defendants that are attributable to the violations alleged herein, or statutory damages in  
4 the amount of up to \$10,000 for each violation of 47 U.S.C. § 605(a), pursuant to 47 U.S.C. §  
5 605(e)(3)(C)(i).

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

8 F. Award DISH Network the greater of its actual damages together with any profits  
9 made by defendants that are attributable to the violations alleged herein, or statutory damages in  
10 the amount of up to \$100,000 for each violation of 47 U.S.C. § 605(e)(4), pursuant to 47 U.S.C.  
11 § 605(e)(3)(C)(i).

12 G. Award DISH Network the greater of its actual damages together with any profits  
13 made by defendants that are attributable to the violations alleged herein, or statutory damages in  
14 the amount of up to \$2,500 for each violation of 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1),  
15 pursuant to 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A).

16 H. Award DISH Network the greater of its actual damages together with any profits  
17 made by defendants that are attributable to the violations alleged herein, or statutory damages in  
18 the amount of \$100 per day for each violation of 18 U.S.C. § 2511(1) or \$10,000, pursuant to 18  
19 U.S.C. § 2520(c)(2).

20 I. Award DISH Network punitive damages afforded by law pursuant to 18 U.S.C. §  
21 2520(b)(2), and in equity for unjust enrichment.

22 J. For an award of DISH Network's costs, reasonable attorneys' fees, and  
23 investigative fees.

24 ...

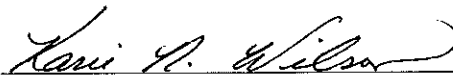
1 K. For pre- and post-judgment interest on all profits and damages granted by this  
2 court in accordance with the law.

3 L. For an accounting and restitution by defendants of all gain, profit, and advantages  
4 derived from defendants' unlawful and unfair business acts and practices.

5 M. For such other and further relief as the court deems just and proper.

6 Dated this 17th day of June, 2010.

7 ALVERSON, TAYLOR  
8 MORTENSEN & SANDERS

9 

10 J. BRUCE ALVERSON, ESQ.

11 Nevada Bar No. 1339

12 KARIE N. WILSON, ESQ.

13 Nevada Bar No. 7957

14 7401 W. Charleston Boulevard

15 Las Vegas, NV 89117

16 702-384-7000 Phone

17 702-385-7000 Fax

18 JOSEPH H. BOYLE (pro hac vice to be filed)

19 joe.boyle@hnbllc.com

20 CHAD M. HAGAN (pro hac vice to be filed)

21 chad.hagan@hnbllc.com

22 HAGAN NOLL & BOYLE LLC

23 Two Memorial City Plaza

24 820 Gessner, Suite 940

Houston, Texas 77024

713-343-0478 Phone

713-758-0146 Fax

n:\bruce.grp\z-client\18789\pleadings\complaint.docx