

1
2
3
4
5
6
7
8
9
10
11
12
13

DLA PIPER US LLP
Roy K. McDonald (State Bar No. 193691)
roy.mcdonald@dlapiper.com
Stephen A. Chiari (State Bar No. 221410)
stephen.chiari@dlapiper.com
153 Townsend Street, Suite 800
San Francisco, California 94107-1957
Telephone: (415) 836-2547
Facsimile: (415) 659-7447

Attorneys for Plaintiffs
ECHOSTAR SATELLITE L.L.C.,
ECHOSTAR TECHNOLOGIES CORPORATION
and NAGRASTAR L.L.C.

E-filing

EMC

CV 07 6124

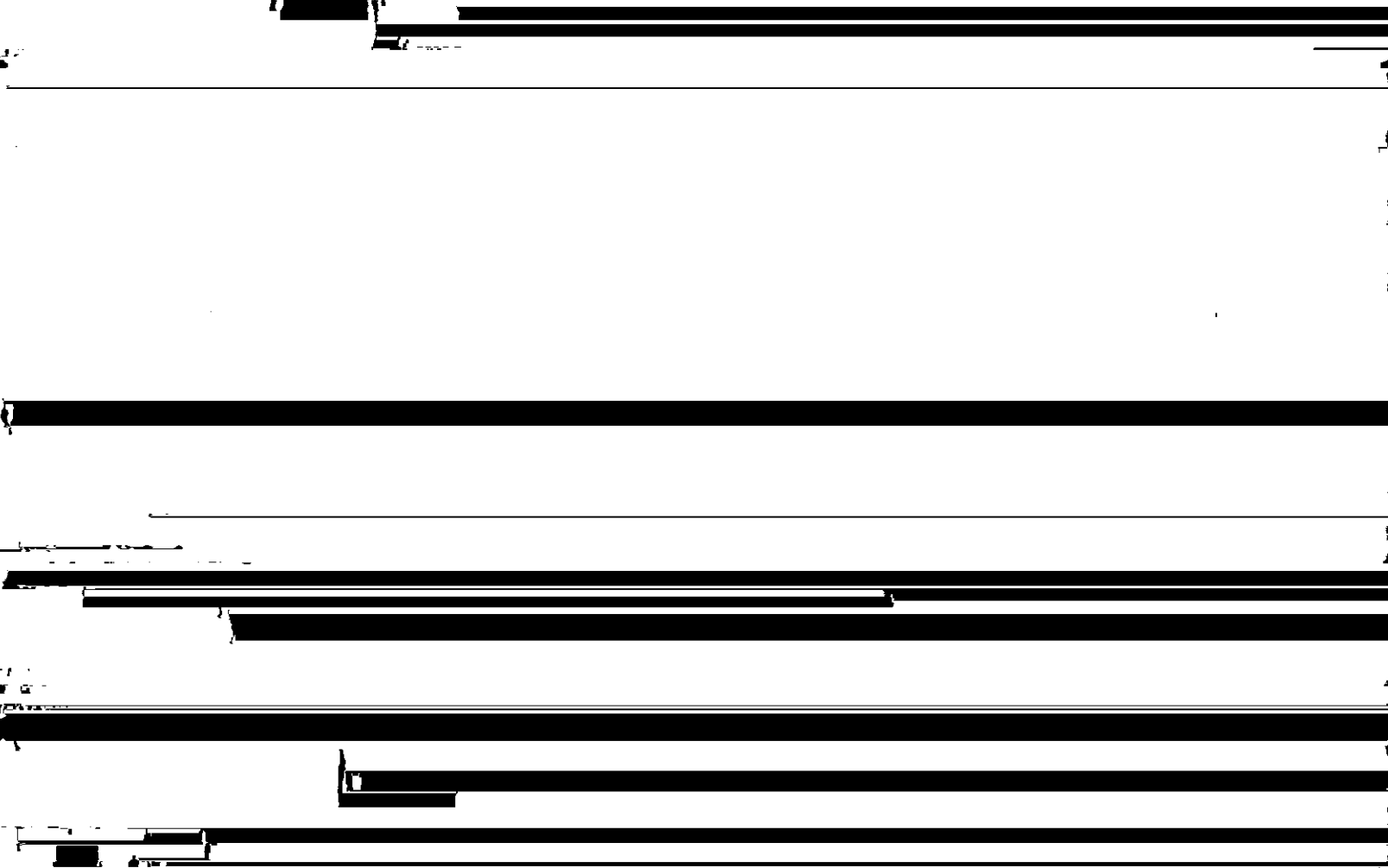
UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ECHOSTAR SATELLITE L.L.C., a
Colorado Limited Liability Company,
ECHOSTAR TECHNOLOGIES



PLAINTIFFS' COMPLAINT FOR:

@ dlapi
FILED
07 DEC -4 AM 11:07
RICHARD W. KING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA



1 Plaintiffs ECHOSTAR SATELLITE L.L.C., ECHOSTAR TECHNOLOGIES
2 CORPORATION (collectively "ECHOSTAR"), and NAGRASTAR L.L.C. ("NAGRASTAR"),
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 ECHOSTAR and NAGRASTAR bring this action against Defendants
7 FREETECH, INC. and DOES 1 through 10 (collectively "Defendants") for unlawfully
8 manufacturing, distributing, and otherwise trafficking in devices, components, and technology
9 intended to facilitate the illegal and unauthorized reception and decryption of ECHOSTAR's
10 subscription and pay-per-view television programming.

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

17 3. ECHOSTAR operates its DBS Programming under the trade name "DISH
18 Network." To provide customers with a variety of Programming channels, ECHOSTAR
19 continues to contract and purchase the distribution rights of copyrighted Programming from
20 providers such as network affiliates, pay and specialty broadcasters, cable networks, motion
21 picture distributors, sports leagues, event promoters, and other content providers.

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

27 5. ECHOSTAR protects DISH Network Programming from unauthorized viewing by
28 using a management and security system ("Security System"), which serves two interrelated

1 functions: (1) subscriber-management—allowing EHOSTAR to “turn on” or “turn off”
2 Programming that a customer ordered, cancelled, or changed; and (2) encryption—preventing
3 individuals or entities who have not purchased DISH Network Programming from viewing it.

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

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

18 PARTIES

19 8. Plaintiff EHOSTAR SATELLITE L.L.C. is a Colorado limited liability company
20 with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado
21 80112.

22 9. Plaintiff EHOSTAR TECHNOLOGIES CORPORATION is a Texas corporation
23 with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado
24 80112.

25 10. Plaintiff NAGRASTAR L.L.C. is a Colorado limited liability company with its
26 principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112.
27 NAGRASTAR is a joint venture between EHOSTAR and the Kudelski Group, a group of
28 companies headquartered in Switzerland.

1 11. Upon information and belief, Defendant FREETECH, INC. ("FREETECH") is a
2 California corporation with its principal place of business located at 469 Littlefield Avenue,
3 South San Francisco, California 94080. The registered agent for FREETECH is Heejoun Jin, 469
4 Littlefield Avenue, South San Francisco, California 94080.

5 12. The true names and capacities of Defendants DOES 1 through 10, whether
6 individual, corporate, associate, or otherwise, are masked by monikers used on the Internet and
7 thus unknown to Plaintiffs at this time. Plaintiffs believe that information obtained in discovery
8 will lead to the identification of each Defendant's true name.

9 13. Upon information and belief, each of the Defendants, including DOES 1 through
10 10, was the agent and/or principal for one another, was acting within the scope of such agency
11 when engaging in the misconduct alleged herein, and is jointly and severally liable for all
12 damages arising as a result thereof.

13 **JURISDICTION AND VENUE**

14 14. This is a civil action predicated upon violations of the Digital Millennium
15 Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Communications Act of 1934, as amended, 47
16 U.S.C. § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.*
17 Therefore, jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331, 1338, 47 U.S.C. §
18 605(e)(3)(A), 17 U.S.C. § 1203, and 18 U.S.C. § 2520(a). The Court has supplemental
19 jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a).

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

26 **PLAINTIFFS' SECURITY SYSTEM**

27 16. A consumer wishing to subscribe to and receive DISH Network Programming
28 must first have the necessary equipment, which consists primarily of: (1) a satellite dish antenna

1 (“dish”); (2) an integrated receiver/decoder (“receiver” or “set-top box”); and (3) a credit card-
2 sized ECHOSTAR Access Card.

3 17. A satellite dish can be mounted on a rooftop, deck railing, or other structure at the
4 subscriber’s home or business. After proper installation, the dish antenna will receive
5 programming signals from one of ECHOSTAR’s satellites, which are then transmitted by wire
6 into the set-top box. The receiver processes and descrambles the incoming signal using the data
7 and encryption technology stored in the ECHOSTAR Access Card. The Access Card is loaded
8 into the receiver through a slot located at the face of the unit.

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

15 19. The ECHOSTAR Access Card is essential to the operation of the set-top box
16 because it contains a secure embedded microprocessor that essentially functions as a small
17 security computer, with secret keys and software that contain technology codes (“Nagra
18 Software”) used to communicate with the receiver and enable the descrambling of DISH Network
19 Programming. The Nagra Software and the security components contained in each set-top box
20 are licensed from NAGRASTAR.

21 20. The Nagra Software within each Access Card is supported by two code segments
22 of memory: (1) Read-Only-Memory (“ROM”); and (2) Electronically Erasable Programmable
23 Read-Only-Memory (“EEPROM”). Generally, the ROM code segment contains the intimate
24 knowledge and information regarding Plaintiffs’ Security System and how it works; whereas the
25 EEPROM code segment contains the secret keys enabling the decryption of ECHOSTAR’s
26 satellite signal.

27 21. The ROM code segment provides detailed instructions and commands to
28 ECHOSTAR Access Cards and set-top boxes in the normal operation of Plaintiffs’ Security

1 System. Access to the proprietary information stored in the ROM code is necessary to unlock the
2 safe containing the secrets to Plaintiffs' Security System.

3 22. The EEPROM code segment stores data and command codes that have been
4 written to ECHOSTAR Access Cards which the ROM code reads from to perform its calculation
5 and operation functions. Moreover, the EEPROM code segment contains secret "transmission"
6 keys and secret "pairing" keys (collectively known as "security keys"). The security keys are
7 used to encrypt and decrypt the communications between the ECHOSTAR Access Card and the
8 set-top box.

9 23. ECHOSTAR communicates with the microprocessor in each Access Card by
10 sending and receiving satellite signals which are routinely updated. The information transmitted
11 to and temporarily stored on the Access Card includes the most recent security keys and software
12 necessary to view DISH Network Programming.

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

17 **THE PIRACY OF DISH NETWORK PROGRAMMING**

18 25. Upon information and belief, satellite pirates reverse engineered the Nagra
19 Software in the ECHOSTAR Access Card. As a result, these pirates ultimately copied and
20 acquired the proprietary information stored within the ROM and EEPROM code segments of the
21 Access Card, and compromised Plaintiffs' Security System. The pirate community (commercial
22 and consumer) used this knowledge to develop various types of devices and technology for the
23 sole purpose of illegally descrambling or "pirating" DISH Network Programming.

24 26. To combat the piracy of DISH Network Programming, Plaintiffs periodically
25 introduce new ECHOSTAR Access Cards that contain updated security codes and software. In
26 addition, Plaintiffs continue to invest in the development and deployment of electronic
27 countermeasures ("ECM") to maintain the integrity of the Security System. An ECM is a
28

1 command transmitted in the stream of data that targets Access Cards, or clones thereof, that are
2 using known modified software code and disables those Access Cards.

3 THE SALE AND USE OF FREE-TO-AIR RECEIVERS FOR SATELLITE PIRACY

4 27. Despite the continuous improvements to Plaintiffs' Security System, satellite
5 piracy continues to proliferate with the ever-growing access and popularity of the Internet. With
6 the Internet as a sword, pirates developed a new way to steal DISH Network Programming by
7 using so-called "free-to-air" receivers ("FTA Receivers"). FTA Receivers are devices that can
8 receive "free-to-air" satellite television signals, which are either not scrambled or scrambled but
9 available free of charge. "Free-to-air" channels do not offer the same type of popular
10 programming found in subscription television packages (e.g. HBO, ESPN, etc.). Instead, "free-
11 to-air" television channels typically include limited ethnic, religious, business, music,
12 information, and advertising content.

13 28. FTA Receivers are similar to the receivers used by ECHOSTAR in that they are
14 set-top boxes, approximately the size of a VCR player, which contain descrambling circuits and
15 software that enables the units to perform designated functions. A variety of FTA Receivers are
16 even equipped with an Access Card reader.

17 29. While FTA Receivers contain many of the same components found in an
18 ECHOSTAR set-top box, the units cannot descramble and receive DISH Network Programming
19 without utilizing the security keys and technology codes found in the Nagra Software (i.e. ROM
20 code segment, EEPROM code segment). Upon information and belief, manufacturers of FTA
21 Receivers developed firmware and components within each unit that will accept and receive
22 illegal pirate software (hereinafter "Pirate Software") that contains the secret keys and codes to
23 Plaintiffs' Security System. Once this technology is downloaded or "flashed" into the FTA
24 Receiver, the unit will illegally receive DISH Network Programming.

25 30. Upon information and belief, the firmware and components within each FTA
26 Receiver that enable the device to accept the download of illegal Pirate Software are (1) a
27 capability that has been designed into each FTA Receiver specifically for Pirate Software; and (2)
28 a capability that has no practical application other than to circumvent Plaintiffs' Security System.

1 31. Commercial pirates acquired, modified, and sold FTA Receivers by: (1) obtaining
2 the FTA Receivers directly from their manufacturer or elsewhere; (2) loading or “flashing” the
3 requisite Pirate Software onto the circuit chips or firmware contained within the FTA Receivers;
4 (3) once “flashed” with the Pirate Software, “testing” the FTA Receivers to ensure the device
5 would receive and descramble DISH Network Programming without authorization from or
6 payment to ECHOSTAR; and (4) ultimately, selling the FTA Receivers to household consumer
7 pirates on the Internet.

8 32. Upon information and belief, commercial pirates recently changed their approach
9 by not actually loading the Pirate Software onto the FTA receivers themselves, but distributing
10 the requisite piracy technology and information to select individuals on websites or Internet
11 discussion “forums” who then offer the Pirate Software to consumers for download. These
12 websites or forums are typically sponsored by many of the commercial pirates, who use this
13 venue to advertise and tout their brand of FTA equipment. This approach, which is prevalent
14 today, permits commercial pirates (including the manufacturers and distributors of FTA
15 Receivers) to assert the misleading claim that they are distributing only “unprogrammed” or
16 “unflashed” piracy devices to consumers.

17 33. In some cases, website forums provide and offer: (1) information and/or
18 instruction, including sources of supply, production information, and product reviews; (2)
19 discussion threads on topics of interest to the piracy community, including software “hacks” or
20 “fixes” designed to restore functionality to ECHOSTAR Access Cards that have been disabled by
21 Plaintiffs’ countermeasures; (3) security keys for DISH Network Programming, which are
22 necessary to unscramble programming from an FTA receiver; (4) piracy or “flashing” software
23 files for download to their users; and (5) links and advertisements to other piracy websites that
24 sell FTA Receivers, Pirate Software, or other piracy devices, components, and technology used to
25 steal DISH Network Programming.

26 34. Successful forum sites can have thousands of members, and are often managed by
27 certain users designated by the operating pirate(s) as “administrators” or “moderators.” These
28 individuals are typically given the authority to manage the content posted on the forum site.

1 Upon information and belief, the distributors of FTA Receivers provide equipment, updated
2 piracy technology, and information to the administrators or moderators of select forums for
3 distribution.

4 35. The distribution, sale, and use of FTA Receivers for piracy pose a serious threat
5 to EHOSTAR and NAGRASTAR. Inasmuch as FTA Receivers are not manufactured or sold
6 by Plaintiffs to receive DISH Network Programming, neither EHOSTAR nor NAGRASTAR
7 can control or regulate the software contained in these devices. As a result, the ECMs
8 traditionally used to combat satellite piracy may not be effective.

9 **DEFENDANTS' WRONGFUL CONDUCT**

10 36. Defendants directly, and through others acting in concert, distribute and promote
11 the sale of "Coolsat" branded FTA Receivers throughout the United States. Upon information
12 and belief, discovery will show that Defendants sold thousands of these FTA Receivers to
13 consumer pirates for the sole purpose of circumventing Plaintiffs' Security System.

14 37. Similar to other FTA Receivers, it is believed that the satellite equipment
15 distributed by Defendants contains computer firmware and components designed to accept the
16 download of Pirate Software created solely for "Coolsat" branded FTA Receivers. Once flashed
17 with this technology, these FTA Receivers can and will illegally receive DISH Network
18 Programming.

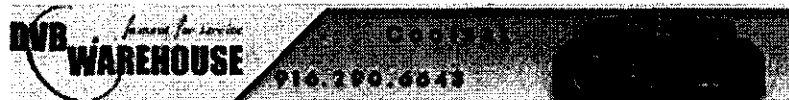
19 38. Defendants import a variety of FTA Receivers from a manufacturer in Asia. Upon
20 information and belief, discovery will show that this manufacturer not only creates the firmware
21 and components within each device, but develops, designs, and updates the requisite Pirate
22 Software with the assistance and support of Defendants.

23 39. Upon information and belief, discovery will show that FTA Receivers accept the
24 download of illegal Pirate Software through internal firmware and components that (1) have been
25 specifically designed to communicate with Pirate Software; and (2) have no commercially
26 significant purpose or use other than to circumvent Plaintiffs' Security System.

27 40. Upon information and belief, discovery will also show that Defendants directly,
28 and through others acting in concert, distribute the updated Pirate Software to select website

1 administrators and moderators, who then disseminate this technology to consumers on the
2 Internet. Because Plaintiffs continue to develop technological measures that effectively control
3 access to the copyrighted Programming on the DISH Network satellite platform, the demand for
4 updated Pirate Software remains constant. As a result, the popularity of pirate websites and
5 discussion forums continues to grow.

6 41. Defendants' authorized dealers purposefully advertise and promote "Coolsat"
7 branded FTA Receivers on several well-known piracy websites. These websites not only provide
8 consumers with illegal Pirate Software, but offer instruction and information used to unscramble
9 and steal DISH Network Programming. Below are exemplars of typical hyperlink advertisements
10 prominently displayed on pirate websites:



14

15

16 42. Upon information and belief, discovery will show that competition within the FTA
17 industry is volatile and market share is contingent upon the immediate availability of updated
18 Pirate Software. Distributors, such as FREETECH, are often pressured to provide consumer
19 pirates with an immediate "fix" to combat a particular countermeasure or ECM utilized by
20 Plaintiffs to prevent the unauthorized reception of DISH Network Programming. FREETECH is
21 considered one of the industry leaders because of its commitment to immediately address the
22 demands of the pirate community.

23 43. Upon information and belief, discovery will show that FREETECH developed the
24 following process to expedite the design, development, and distribution of Pirate Software: (1)
25 Defendants continuously monitor and intercept Plaintiffs' encrypted satellite signals to determine
26 the deployment of an ECM; (2) Defendants immediately solicit information identifying the
27 countermeasure commands transmitted in a particular ECM; (3) after Defendants acquire the
28 requisite ECM data or "log" of coded commands (typically in "hexadecimal" format),

1 FREETECH then sends the information directly to coders in Asia; (4) the coders analyze the data
2 and develop a “fix” or “patch” to the ECM; (5) the updated Pirate Software is then sent from the
3 coders directly to FREETECH for testing; (6) if the updated Pirate Software effectively counters
4 the ECM by allowing the user to circumvent Plaintiffs’ Security System, FREETECH sends the
5 “fix” to an individual known in the pirate community as “David Smith,” “Tecknofreak,” and
6 “Matchstick” (collectively “Smith”); (7) Smith disseminates the updated Pirate Software through
7 a fictitious entity or group of individuals known as the “Norwest Group” to several pirate
8 websites, including www.fortecfiles.com, www.abadss.com, and www.f2atv.com.

9 44. Aside from the aforementioned design, development, and distribution, it is
10 believed that FREETECH also utilizes Pirate Software to conduct diagnostic evaluations of FTA
11 Receivers returned to FREETECH for reported warranty repair. Upon information and belief,
12 discovery will show that FREETECH purposefully “flashes” or loads the most recent version of
13 Pirate Software onto returned “Coolsat” FTA Receivers to determine why a particular unit is
14 reportedly unable to receive DISH Network Programming. Once repaired, the Pirate Software is
15 deleted from the FTA Receiver and the unit is returned to the customer, who is then directed to,
16 or provided by Defendants, the updated Pirate Software for download.

17 CLAIMS FOR RELIEF

18 COUNT I

19 **(Manufacture of and Traffic in Signal Theft Devices, Components, and Technology in** 20 **Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1))**

21 45. Plaintiffs incorporate by reference paragraphs 1 through 44 as if set forth herein.

22 46. Defendants were and are actively engaged in the business of manufacturing,
23 importing, offering to the public, providing, or otherwise trafficking in the sale of illegal pirate
24 devices, components, and technology in violation of the Digital Millennium Copyright Act
25 (“DMCA”), 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1).

26 47. The FTA Receivers and corresponding Pirate Software provided by Defendants
27 are: (1) designed or produced by Defendants primarily for the circumvention of Plaintiffs’
28 Security System—a technological measure that effectively controls access to, copying and

1 distribution of, copyrighted works; (2) made available by Defendants despite having no limited
2 commercially significant purpose or use other than to circumvent Plaintiffs' Security System;
3 and/or (3) marketed by Defendants, or through others acting in concert, with knowledge that the
4 devices, components, and technology are used to circumvent Plaintiffs' Security System.

5 48. Defendants were and are manufacturing, importing, offering to the public,
6 providing, or otherwise trafficking "Coolsat" branded FTA Receivers and corresponding Pirate
7 Software with knowledge that these devices, components, and technology are used to circumvent
8 and defeat Plaintiffs' conditional access technological measures that protect the copyrighted
9 works on the DISH Network satellite platform.

10 49. Defendants' actions that constitute violations of the DMCA were performed
11 without the permission, authorization, or consent of ECHOSTAR, NAGRASTAR, or any owner
12 of copyrighted Programming broadcast on the DISH Network platform.

13 50. Defendants violated sections 1201(a)(2) and 1201(b)(1) of the DMCA willfully
14 and for purposes of commercial advantage or private financial gain.

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

18 **COUNT II**

19 **(Facilitating the Unauthorized Decryption and Reception of Satellite Signals** 20 **in Violation of the Communications Act, 47 U.S.C. § 605(a))**

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

22 53. Defendants were and are assisting others, namely those purchasing "Coolsat"
23 branded FTA Receivers and downloading the corresponding Pirate Software from websites, to
24 intercept and receive ECHOSTAR's encrypted satellite transmissions without authorization and
25 for their own benefit in violation of 47 U.S.C. § 605(a).

26 54. Defendants were and are assisting, directly or indirectly, with the design,
27 manufacture, development, assembly, modification, solicitation, and/or distribution of "Coolsat"
28 branded FTA Receivers and corresponding Pirate Software with knowledge, or having reason to

1 know, that such devices and technology are used primarily to assist in the unauthorized
2 interception and decryption of direct-to-home satellite services in violation of 47 U.S.C. § 605(a).

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

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

8 **COUNT III**

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

11 57. Plaintiffs incorporate by reference paragraphs 1 through 56 as if set forth herein.

12 58. Defendants were and are engaged in the business of designing, manufacturing,
13 developing, assembling, modifying, importing, exporting, selling, or otherwise distributing
14 "Coolsat" branded FTA Receivers and corresponding Pirate Software to facilitate the illegal use
15 and reception of ECHOSTAR's encrypted satellite transmissions without authorization in
16 violation of 47 U.S.C. § 605(e)(4).

17 59. Defendants were and are assisting, directly or indirectly, with the design,
18 manufacture, development, assembly, modification, solicitation, and/or distribution of "Coolsat"
19 branded FTA Receivers and the corresponding Pirate Software with knowledge, or having reason
20 to know, that such devices and technology were and are used primarily to assist in the
21 unauthorized interception and decryption of direct-to-home satellite services in violation of 47
22 U.S.C. § 605(e)(4).

23 60. Defendants violated 47 U.S.C. § 605(e)(4) of the Communications Act willfully
24 and for the purpose of direct or indirect commercial advantage or private financial gain.

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

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

COUNT IV

(Unauthorized Interception of Electronic Communications in Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2520(a))

62. Plaintiffs incorporate by reference paragraphs 1 through 61 as if set forth herein.

63. Defendants were and are intentionally intercepting ECHOSTAR's encrypted satellite transmissions in violation of the Electronic Communications Privacy Act ("Wiretap Act"), 18 U.S.C. § 2520(a), by using "Coolsat" branded FTA Receivers, components, and corresponding Pirate Software, which is prohibited by section 2511(1)(a) of the Wiretap Act.

64. Defendants knew that the interception of ECHOSTAR's encrypted satellite signals was and is illegal and prohibited.

65. Defendants violated sections 2511(1)(a) and 2520(a) of the Wiretap Act for a tortious or illegal purpose, or for purposes of direct or indirect commercial advantage or private financial gain.

66. 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 the alleged provisions of the Wiretap Act.

COUNT V

(Unfair Competition in Violation of California Business & Professions Code § 17200)

67. Plaintiffs incorporate by reference paragraphs 1 through 66 as if set forth herein.

68. Defendants' promotion, distribution, and provision of piracy devices, components, and technology which are primarily designed to circumvent Plaintiffs' Security System and steal DISH Network Programming constitute unlawful and unfair business acts and practices within the meaning of California Business and Professions Code § 17200 *et seq.*

69. Defendants' unlawful business acts and practices, as alleged herein, violate provisions of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Communications Act of 1934, as amended, 47 U.S.C. § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.*

///

1 ECHOSTAR. The amount of profits unjustly realized by Defendants cannot be readily
2 ascertained by ECHOSTAR without an accounting of Defendants' business records.

3 77. Unless permanently restrained and enjoined, Defendants' misconduct has and will
4 continue to unjustly enrich Defendants and cause further damage to ECHOSTAR in an amount to
5 be proven at trial.

6 **PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiffs ECHOSTAR and NAGRASTAR seek judgment against
8 Defendants as follows:

9 A. For a grant of permanent injunctive relief restraining and enjoining Defendants,
10 and their employees, agents, representatives, attorneys, and all persons acting or claiming to act
11 on their behalf or under their direction or authority, and all persons acting in concert or in
12 participation with them, from:

13 (1) offering to the public, providing, or otherwise trafficking in any FTA
14 Receivers, Pirate Software, or any other device, component, or technology, or part thereof,
15 through the www.fortecfiles.com, www.abadss.com, and www.f2atv.com websites, any other
16 Internet website, or in any other way that:

17 (a) is primarily designed or produced for the purpose of circumventing
18 Plaintiffs' Security System, including the encryption and access control protection contained in
19 the software on ECHOSTAR's Access Cards, or any other technological measure adopted by
20 Plaintiffs that effectively controls access to copyrighted Programming on the DISH Network
21 platform;

22 (b) have only a limited commercially significant purpose or use other
23 than to circumvent Plaintiffs' Security System, including the encryption and access control
24 protection contained in the software on ECHOSTAR's Access Cards, or any other technological
25 measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on the
26 DISH Network platform;

27 (c) is knowingly marketed by Defendants and/or others acting in
28 concert with Defendants for use in circumventing Plaintiffs' Security System, including the

1 encryption and access control protection contained in the software on ECHOSTAR's Access
2 Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to
3 copyrighted Programming on DISH Network; and

4 (2) assembling, modifying, selling, and/or distributing any FTA Receivers or
5 Pirate Software knowing or having reason to know that such device or software is primarily of
6 assistance in the unauthorized decryption of direct-to-home satellite services through the
7 www.fortecfiles.com, www.abadss.com, and www.f2atv.com websites, any other Internet
8 website, or in any other way; and

9 (3) assisting others in receiving (including assistance offered by providing
10 hypertext links or banner advertising) ECHOSTAR's electronic communications without
11 ECHOSTAR's authorization through the www.fortecfiles.com, www.abadss.com, and
12 www.f2atv.com websites, any other Internet website, or in any other way.

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

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

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

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

1 amount of up to \$2,500 for each violation of 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1), pursuant to
2 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A).

3 F. Award Plaintiffs the greater of its actual damages together with any profits made
4 by Defendants that are attributable to the violations alleged herein, or statutory damages in the
5 amount of \$100 per day for each violation of 18 U.S.C. § 2511(1) or \$10,000, pursuant to 18
6 U.S.C. § 2520(c)(2).

7 G. Award Plaintiffs punitive damages afforded by law pursuant to 18 U.S.C. §
8 2520(b)(2), and in equity for unjust enrichment.

9 H. For an accounting and restitution by Defendants of all gain, profit, and advantages
10 derived from Defendants' unlawful and unfair business acts and practices.

11 I. For an award of Plaintiffs' costs, reasonable attorneys' fees, and investigative fees.

12 J. For pre- and post-judgment interest on all profits and damages granted by this
13 Court in accordance with the law.

14 K. For such other and further relief as the Court deems just and proper.

15 DATED: December 3, 2007

Respectfully submitted,

16 DLA PIPER US LLP

17
18 By: 
19 ROY K. McDONALD
STEPHEN A. CHIARI

20 Attorneys for Plaintiffs
21 ECHOSTAR SATELLITE L.L.C.,
22 ECHOSTAR TECHNOLOGIES CORPORATION
23 and NAGRASTAR L.L.C.
24
25
26
27
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


DEMAND FOR JURY TRIAL

Plaintiffs ECHOSTAR SATELLITE L.L.C., ECHOSTAR TECHNOLOGIES CORPORATION, AND NAGRASTAR L.L.C., by their undersigned counsel, hereby demand a trial by jury in this action.

DATED: December 3, 2007

Respectfully submitted,

DLA PIPER US LLP

By: 

ROY K. McDONALD
STEPHEN A. CHIARI

Attorneys for Plaintiffs
ECHOSTAR SATELLITE L.L.C.,
ECHOSTAR TECHNOLOGIES CORPORATION
and NAGRASTAR L.L.C.