

1 T. WADE WELCH & ASSOCIATES
2 Chad M. Hagan (*pro hac vice*)
3 2401 Fountainview, Suite 700
4 chagan@twlaw.com
5 Houston, Texas 77057
6 Telephone: (713) 952-4334
7 Facsimile: (713) 952-4994

8 DLA PIPER US LLP
9 David A. Grenardo (State Bar No. 223142)
10 Cynthia A. Ricketts (*pro hac vice*)
11 david.grenardo@dlapiper.com
12 cindy.ricketts@dlapiper.com
13 1999 Avenue of the Stars, 4th Floor
14 Los Angeles, CA 90067
15 Telephone: (310) 595-3031
16 Facsimile: (310) 595-3331

17 Attorneys for Plaintiffs
18 ECHOSTAR SATELLITE CORP., et al.

19 **UNITED STATES DISTRICT COURT**
20 **CENTRAL DISTRICT OF CALIFORNIA**
21 **SOUTHERN DIVISION**

22 ECHOSTAR SATELLITE
23 CORP., et al.,

24 Plaintiffs/
25 Counterclaim
26 Defendants,

27 v.

28 NDS GROUP PLC, et al.,

Defendants/
Counterclaim
Plaintiffs.

No. SA CV 03-950 DOC(JTL)

**PLAINTIFFS' PROPOSED
FINDINGS OF FACT AND
CONCLUSIONS OF LAW RE:
CALIFORNIA BUSINESS AND
PROFESSIONS CODE § 17200**

TABLE OF CONTENTS

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

Page No.

I. PROPOSED FINDINGS OF FACT 2

II. DISCUSSION AND CONCLUSIONS OF LAW 14

 A. Defendants Have Engaged in Unlawful Business Practices..... 14

 B. Defendants Have Engaged In Unfair Business Practices..... 16

 C. Plaintiffs Are Entitled To Restitution And An Injunction..... 18

1 **TABLE OF AUTHORITIES**

2 **CASES**

3 Page Nos.

4 *A-C Co. v. Security Pacific Nat. Bank,*
173 Cal.App.3d 462, 219 Cal.Rptr. 62 (Dist. 4 1986) 14

5 *Cel-Tech Communications, Inc. v. Los Angeles Cellular Tele. Co.,*
6 20 Cal. 4th 163 (1999) 13, 15, 16

7 *Citizens for a Better Environment-California v. Union Oil of Cal.,*
8 996 F. Supp. 934 (N.D. Cal. 1997) 13

9 *Farmers Ins. Exch. v. Superior Court,*
2 Cal. 4th 377 (1992) 13

10 *Kasky v. Nike, Inc.,*
11 27 Cal. 4th 939 (2002) 13

12 *Klein v. Earth Elements, Inc.,*
59 Cal. App. 4th 965 (1997) 14

13 *Mattel, No. CV 05-2727 NM (RNBx),*
14 2005 WL 5894689 (C.D. Cal. Aug. 26, 2005) 15, 16

15 *Nat'l Rural Telecom. Coop. v. DirecTV, Inc.,*
319 F. Supp. 2d 1059 (C.D. Cal. 2003) 13

16 *No. C-07-0635 JCS,*
17 2007 WL 1455903 (N.D. Cal. May 16, 2007) 16

18 *People v. Baker,*
126 Cal. App. 4th 463 (Cal. App. 5th Dist. 2005) 18

19 *People v. Beaumont Inv., Ltd.,*
20 111 Cal. App. 4th 102, 3 Cal. Rptr. 3d 429 (2003) 18

21 *People v. E.W.A.P. Inc.,*
106 Cal. App. 3d 315 (1980) 14, 19

22 *People v. Fremont Life Ins. Co.,*
104 Cal. App. 4th 508 (2003) 13

23 *People v. Toomey,*
24 157 Cal. App. 3d 1 (1985) 18, 19

25 *Podolsky v. First Healthcare Corp.,*
26 50 Cal. App. 4th 632 (1996) 14

27 *Southwest Marine, Inc. v. Triple A Machine Shop, Inc.,*
720 F. Supp. 805 (N.D. Cal. 1989) 13

28

1 *United States v. Traylor*,
2 978 F.2d 1131 (9th Cir. 1992) 17

3 **STATUTES**

4 Cal. Bus. & Prof. Code § 17203 17, 18, 19
5 Communications Act of 1934, 47 U.S.C. § 605(a)..... 14, 19
6 Fed. R. Civ. P. 52 1

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Plaintiffs EchoStar Satellite L.L.C. f/k/a EchoStar Satellite Corporation,
2 EchoStar Technologies Corporation, and NagraStar L.L.C. (collectively,
3 “Plaintiffs” or “EchoStar”) respectfully submit these proposed findings of fact and
4 conclusions of law regarding the liability of Defendants NDS Group PLC and NDS
5 Americas, Inc. (collectively, “Defendants” or “NDS”) under California Business
6 and Professions Code § 17200 and remedies thereunder, pursuant to Fed. R. Civ. P.
7 52.

8 **I. PROPOSED FINDINGS OF FACT**

9 Based upon the evidence presented at trial, the Court hereby makes the
10 following findings of fact:

11 **Plaintiffs and Defendants and Related Entities Compete** 12 **in the U.S. Satellite Television Market.**

13 1. EchoStar is one of the largest satellite providers in the United States
14 and offers about 500 television channels with various subscription packages to
15 consumers. (Ergen Trial Testimony 4/9/08, Vol. 5 p. 8:18-9:20.)

16 2. Under the name DISH Network, EchoStar provides programming to
17 paying subscribers. (*Id.* pp. 7:17-8:10, 8:18-9:20.)

18 3. EchoStar generally pays the programming companies a fee for each
19 subscriber to which it broadcasts the programming. (*Id.*)

20 4. EchoStar contracts with programming companies such as Disney,
21 which owns ESPN and the Disney Channel. (*Id.* p. 9:9-20.)

22 5. EchoStar also has its own copyrighted programming that it broadcasts
23 on the DISH Network to paying subscribers. (*Id.* p. 10:20-23.)

24 6. EchoStar makes a substantial investment in encryption systems or
25 conditional access systems (“CAS”) to prevent people from taking its satellite
26 signals without authorization. (*Id.* p. 11:8-22.)

27 7. A CAS allows a customer to receive only channels for which the
28 customer pays by sending a key through the satellite to the “SmartCard” in the

1 customer's set-top box; the key unlocks the channels for which the customer has
2 paid (and does not unlock the channels for which the customer has not paid). (*Id.* p.
3 13:17-12; Lenoir Trial Testimony 4/10/08, Vol. 1, p. 52:22-53:4.)

4 8. Plaintiff NagraStar is a joint venture of EchoStar and the Kudelski
5 Group in Switzerland. (Ergen Trial Testimony 4/9/08, Vol. 5 p. 50:21-p. 51:7.)

6 9. NagraStar provides the SmartCards used in EchoStar's CAS, as well as
7 security-related and maintenance services to EchoStar. (Lenoir Trial Testimony
8 04/10/08, Vol. 1, pp. 52:22-53:4; 55:10-15.)

9 10. Defendant NDS also provides CASs and is the biggest competitor of
10 the Kudelski Group. (*Id.* p. 59:8-11.)

11 11. NDS has 32% of the market and NagraStar has 30% of the market.
12 (*Id.* p. 60:6-8.)

13 12. At all times relevant to this lawsuit, NDS provided DirecTV's CAS in
14 the United States. (Shkedy Trial Testimony 04/10/08, Vol. 3, p. 10:20-11:1; Dov
15 Rubin Trial Testimony 4/22/08, Vol. 1, p. 13:20-24.)

16 13. DirecTV was NDS's largest customer in the United States. (Dov
17 Rubin Trial Testimony 4/22/08, Vol. 1, p. 14:6-11.)

18 **Afraid of Losing Their Largest Customer, Defendants Engaged in a Series of**
19 **Schemes to Hack and Pirate Satellite Television Providers.**

20 14. In 1997-2002, Defendants experienced significant problems with the
21 circumvention of their encryption technology (*i.e.*, CAS) by pirates in both the
22 United States and Europe. (Shkedy Trial Testimony 04/10/08, Vol. 3, p. 10:20-
23 11:1; Dov Rubin Trial Testimony 4/17/08, Vol. 1, pp. 68:11-17; 78:15-79:1; Norris
24 Trial Testimony 4/16/08, Vol. 4, p. 24:6-25:5; Tarnovsky Trial Testimony
25 04/23/08, Vol. 1 p. 58:9-15.)

26 15. As a result, DirecTV was considering other suppliers, including
27 NagraStar, and NDS was afraid it was going to lose DirecTV, its largest customer.
28 (Dov Rubin Trial Testimony 4/22/08, Vol. 1, p. 58:9-19; Andre Kudelski Trial

1 Testimony 5/6/08, Vol. 1, p. [trans. not yet avail.]

2 16. At the same time, NDS sought EchoStar as a customer. (Dov Rubin
3 Trial Testimony 4/22/08, Vol. 1, p. 77:25-78:17.)

4 17. To prevent losing DirecTV as a customer, NDS developed a strategy
5 of co-opting the pirates; in other words, “pay[ing] them not to pirate your system
6 and hope they pirate your competition.” (TR EX 360.)

7 18. NDS was aware that it was helpful to its marketing efforts to tell
8 customers that its competitor’s CAS had been hacked or compromised. (Segoly
9 Trial Testimony 04/11/08, Vol. 2, p. 82:25-83:7 (“If competitor is hacked or
10 compromised, yes, it is important for marketing and sales.”), p. 85:1-5 (talking
11 about EchoStar’s system: “if it’s hacked, and if it’s available on the Internet, and if
12 there are devices out there, then yes, it is important.”); Dov Rubin Trial Testimony
13 4/22/08, Vol. 1, p. 26:18, 27:2-33:16; TR EX 1270.)

14 19. As part of the company strategy, starting in 1997, NDS initiated efforts
15 to recruit and employ satellite hackers Christopher Tarnovsky (“Tarnovsky”) and
16 Oliver Kommerling (“Kommerling”), whom Defendants believed to be a major
17 source of their piracy problems. (Norris Trial Testimony 04/17/08, Vol. 2, p. 73:3-
18 20.)

19 20. Indeed, Tarnovsky admitted that prior to going to work for NDS, he
20 was engaged in compromising NDS’s CAS, which allowed DirecTV programming
21 to be stolen. (Tarnovsky Trial Testimony 04/23/08, Vol. 1, pp. 52:14-21, 58:13-14;
22 Vol. 3, p. 55:25-58:5.)

23 21. Tarnovsky freely admitted that he was a “hacker.” (*Id.* p. 55:2-4; TR
24 EX 6-A (“My name is Chris Tarnovsky, and I’m a hacker.”).) Specifically, Ron
25 Ereiser (“Ereiser”) hired Tarnovsky to hack the DirecTV system and paid
26 Tarnovsky \$20,000. (Tarnvosky Trial Testimony 04/23/08, Vol. 3 p. 58:15-59:5.)

27 22. Tarnovsky worked with Ereiser for approximately nine months before
28 going to work for NDS as discussed further below. (*Id.* p. 60:1-5.)

1 23. NDS was aware of Tarnovsky’s and Kommerling’s hacking activities
2 – in fact, NDS recruited Tarnovsky and Kommerling because NDS considered them
3 to be the “two best hackers in the world,” even though they considered these
4 hacking activities to be illegal. (Norris Trial Testimony 04/16/08, Vol. 4, p. 23:23-
5 24:5; Dov Rubin Trial Testimony 4/22/08, Vol. 1, p. 15:3-6; Segoly Trial
6 Testimony 04/11/08, Vol. II, p. 73:18-23; Hasak Trial Testimony 05/01/08, Vol. 1,
7 p. 77:10-24.).

8 24. When NDS hired Tarnovsky, NDS knew that Tarnovsky had
9 relationships with known pirates and that his friend Alan Menard (“Menard”) was
10 using a pirate card Tarnovsky had developed to hack DirecTV. (Tarnovsky Trial
11 Testimony 04/23/08, Vol. 3, p. 36:25-37:7.)

12 25. NDS also knew that there was a risk that Tarnovsky would continue to
13 engage in his illegal hacking activities. (Dov Rubin Trial Testimony 4/22/08, Vol.
14 1, p. 15:3-12; Segoly Trial Testimony 4/11/08, Vol. 2, pp. 77:22-78:2, 78:13-16.)

15 26. NDS nonetheless hired Tarnovsky. (Dov Rubin Trial Testimony
16 4/22/08, Vol. 1, p. 15:3-12.)

17 27. NDS set up a lab for Tarnovsky in his house and allowed Tarnovsky to
18 work from his house during the nearly ten (10) years he was a NDS employee.
19 (Tarnovsky Trial Testimony 4/23/08, Vol. 2, p. 3:4-9; Vol. 3, p. 23:2-9 (house was
20 an “NDS-equipped lab”); Hasak Trial Testimony 5/1/08, Vol. 1, p. 22:18-23:12
21 (NDS installed an alarm to secure lab in Tarnovsky’s home).)

22 28. When NDS hired Tarnovsky, they paid him \$65,000 a year, \$14,000 in
23 moving expenses, and a \$10,000 loan that could be forgiven in two years.
24 (Tarnovsky Trial Testimony 04/25/08, Vol. 3, p. 63:8-13.)

25 **Defendants Hacked Plaintiffs’ CAS for Competitive Advantage,**
26 **Not to Improve Their Own System.**

27 29. Defendants “reversed engineered” and “hacked” Plaintiffs’ security
28 system at Defendants’ research laboratory in Haifa, Israel over a period of six (6)

1 months. (Shkedy Trial Testimony 04/10/08, Vol. 2, p. 57:13-19; *see* TR EX 2-A
2 (Initial Draft of Headend Report); TR EX 98 (Headend Report); Dov Rubin Trial
3 Testimony 4/17/08, Vol. 1, pp. 74:3-74:15, 75:18-76:24; Hasak Trial Testimony
4 5/1/08, Vol. 1, p. 71:18-21.)

5 30. Defendants' engineers Zvi Shkedy and David Mordinson extracted the
6 proprietary ROM and EEPROM codes from the microprocessor of one of
7 Plaintiffs' access cards and analyzed the code to identify weaknesses and
8 vulnerabilities (which was the purpose of the hacking). (Shkedy Trial Testimony
9 04/10/08, Vol. 2, p. 57:13-19.)

10 31. Mordinson and Shkedy traveled to New Jersey to log data needed to
11 complete the hack. (*Id.* p. 23:15-24:17.)

12 32. Reuven Hasak, one of the senior officers of NDS at the time, set
13 Mordinson and Shkedy up with someone in New Jersey so they could log
14 communications between a set-top box and the Smart Card. (*Id.*)

15 33. Mordinson and Shkedy later traveled to Windsor, Canada, via
16 Cleveland and Baltimore, to successfully test the hack in someone's basement.
17 (Shkedy Trial Testimony 04/10/08, Vol. 3, pp. 25:3-8, 75:12-16; Mordinson Trial
18 Testimony 04/11/08, Vol. 1, pp. 32:6-11, 33:2-12, 35:15-36:1, 36:9-14; Vol. 2 at
19 p. 32:18-33:5.)

20 34. Defendants then prepared a written report that described, in detail: (1)
21 the secret characteristics Defendants discovered in Plaintiffs' microprocessor, (2)
22 the technique Defendants developed to exploit those characteristics, and (3) the
23 process to effectuate a commercial hack of Plaintiffs' encryption system in the
24 United States. (Shkedy Trial Testimony 04/10/08, Vol. 3, p. 19:17-19; Mordinson
25 Trial Testimony 4/10/08, [SPEC] VOL., p. 42:25-16.)

26 35. This report was called the "Headend Report." (Shkedy Trial
27 Testimony 04/10/08, Vol. 3, pp. 7:1-6, 8:5-8, 19:17-19; Mordinson Trial Testimony
28

1 04/11/08, Vol. No. 1, p. 5:17-25; TR EX 2A (Initial Draft Headend Report dated
2 10/27/98); TR EX 98 (final Headend Report).)

3 36. The Headend Report is a “how to” manual for how to break the CAM
4 for the EchoStar system. (Avi Rubin Trial Testimony 4/16/08, Vol. 2, p. 72:5-14.)

5 37. It describes what is in various memory locations, and it gives the code
6 for a message that can be used to run the attackers’ code on the card by exploiting
7 certain vulnerabilities. (*Id.* p. 72:5-14.)

8 38. Importantly, there is nothing in the Headend Report about improving
9 the robustness of Defendants’ own product. (Avi Rubin Trial Testimony 4/16/08,
10 Vol. 3, p. 27:11-28:12.)

11 39. Indeed, the Headend Report does not contain a single section
12 describing how Defendants could use the hacked methodology and the information
13 they learned from the hack of Plaintiffs’ security system to improve Defendants’
14 technology. (TR EX 98 (Headend Report).)

15 40. In fact, the ST Thomson chip ST16CF54 CPU, which is the
16 microprocessor chip in Plaintiffs’ SmartCard and the subject of the Headend
17 Report, was never a chip that NDS used. (Shkedy Trial Testimony 04/10/08, Vol.
18 3, pp. 9:18-10:3, 10:9-19; TR EX 2-A (Initial Draft of Headend Report) at p. 11;
19 TR EX 98 (Headend Report).)

20 41. Knowing the structure of the fields of the memory code in Plaintiffs’
21 access card from ST Thomson did not make NDS’s security technology any more
22 secure. (Shkedy Trial Testimony 04/10/08, Vol. 3, p. 27:2-5.)

23 42. The hack of Plaintiffs’ security system was not done to combat the
24 piracy that DirecTV (and thus NDS) was suffering. (Shkedy Trial Testimony
25 04/10/08, Vol. 3, p. 10:20-11:1.)

26 43. Rather, the Headend Report “teaches anyone that reads it how to create
27 a 3M hack of the EchoStar access cards.” (Shkedy Trial Testimony 04/10/08, Vol.
28 3, p. 28:6-9; TR EX 98 (Headend Report).)

1 44. The Headend Report thus describes how a satellite hacker, or pirate,
2 can view EchoStar’s signals without paying for them. (Shkedy Trial Testimony
3 04/10/08, Vol. 3, p. 13:9-13; TR EX 2-A (Initial Draft of Headend Report, p. 13, ¶
4 3.5.2); TR EX 98 (Headend Report).)

5 45. Indeed, the Headend Report expressly states, “This is a classic 3M
6 hack. The subscriber subscribing to a basic package of service for a minimal
7 possible charge can view any services, excluding PPV, even if he/she is not
8 authorized to view them.” (Shkedy Trial Testimony 04/10/08, Vol. 3, p. 12:23-
9 13:5; TR EX 2-A (Initial Draft of Headend Report, p. 13, ¶ 3.5.2); TR EX 98
10 (Headend Report).)

11 **Defendants Provided the Headend Report, or Portions of It, to**
12 **Tarnovsky to Facilitate the Piracy of EchoStar Cards.**

13 46. Defendants did not keep Headend Report confidential. Instead, NDS
14 gave the report to Kommerling. (Shkedy Trial Testimony 04/10/08, Vol. 3, p. 19:3-
15 9.)

16 47. Additionally, Tarnovsky had a number of “technical exchanges” with
17 the engineers in Haifa, Israel and saw the Headend Report at one of the “technical
18 exchanges” with Mordinson. (Tarnovsky Trial Testimony 04/23/08, Vol. 3, p.
19 11:5-14.)

20 48. Mordinson also flew to California and showed Tarnovsky portions of
21 the Headend Report. (*Id.* p. 11:5-13:24).

22 49. When asked direct questions as to the timing of when he saw the
23 Headend Report, Tarnovsky provided inconsistent answers: at trial, he attempted to
24 testify that he was certain he saw the Headend Report after the December 2000
25 postings (*Id.*, p. 17:17-18:8); at his deposition, Tarnovsky said that it was more
26 likely than not that he saw the Headend Report in 1999; and at several other points,
27 Tarnovsky said it was in 2001 after the December 2000 posting; at one point,
28 Tarnovsky also said that he saw the Headend Report during the “P3 era.” (*Id.*, p.

1 16:25-17:11.)

2 50. However, it is clear that Tarnovsky had access to the Headend Report
3 as early as March 1999. For example, March 28, 1999, Tarnovsky e-mailed to Jan
4 Saggiori portions of EchoStar's ROM and the Confidential User Manual from the
5 e-mail address von@metro2000.net. (Saggiori Trial Testimony 04/16/08, Vol. 1, p.
6 41:17-42:7; TR EX 2002 (e-mail from von@metro2000.net); Tarnovsky Trial
7 Testimony 04/23/08, Vol. 3, p. 13:16-23.)

8 51. Tarnovsky admitted that von@metro2000.net was one of the e-mail
9 addresses that he used. (*Id.*, p. 13:16-23.)

10 52. The March 28, 1999 e-mail from von@metro2000.net has the file
11 name "16cf54.asc," which corresponds to the ST Thomason 16cf54 chip in
12 Plaintiffs' SmartCards (and the chip that was the subject of Defendants' hack). (*Id.*
13 p. 14:17-15:9; TR EX 2002 p. 5.)

14 **Tarnovsky Posted the**
15 **EchoStar Code on the Internet.**

16 53. There are many indications that Tarnovsky posted the EchoStar code
17 contained in the Headend Report on the Internet on behalf of NDS.

18 54. For example, "Nipper," a term that Defendants found in the EchoStar
19 code during their hack, was the alias used to post the code on the Internet.
20 (Mordinson Trial Testimony 4/11/08, Vol. 2, p. 50:1-6).

21 55. The code was posted on the DR7 website, which belonged to Menard;
22 Menard also worked with Tarnovsky to pirate DirecTV. (Menard Trial
23 Designations, pp. 111:18-24, 127:25-128:08.)

24 56. Tarnovsky frequently visited DR7 while working for NDS.
25 (Tarnovsky Trial Testimony 04/23/08, Vol. 2, p. 19:23-20:6; Norris Trial
26 Testimony 4/16/08, Vol. 4, p. 27:10-14.)

27 57. NDS was aware of Tarnovsky's relationship with Menard when NDS
28 hired Tarnovsky. (Tarnovsky Trial Testimony 04/23/08, Vol. 4, pp. 16:22-25,

1 17:1-8 (“Menard was running probably the largest pirate/hacker website for
2 satellite-related pirate activities in the world.”).)

3 58. In October 2000, Defendants instructed Tarnovsky to get NDS an
4 account on www.pirateden.com. (TR EX 42; Tarnovsky Trial Testimony 04/23/08,
5 Vol. 4, p. 66:10-15.)

6 59. The account was registered using the e-mail address
7 ChrisVon@s4interpass.com. (TR EX 351.)

8 60. Tarnovsky used the alias “Von” to post information on Menard’s
9 website DR7. (Tarnovsky Trial Testimony 04/23/08, Vol. 2, p. 20:18-23.)

10 61. The screen name used for this account was “NiPpEr2000.” (TR EX
11 351; TR EX 354; TR EX 39.)

12 62. Tarnovsky has been linked to the alias “Nipper” through an Internet
13 Crimes Group (“ICG”) report. Tarnovsky used aliases “Von” “biggun,” “BG,”
14 “shrimp,” “Geo,” “Geoll,” “ChristoGeo,” “Chris Berry,” “Chris Geo,” and “Arthur
15 Von Neuman,” all of which are listed on the ICG Report. (Norris Trial Testimony
16 4/17/08, Vol. 2, pp. 77:2-8, 78:3-12; Tarnovsky Trial Testimony 04/23/08, Vol. 2,
17 p. 56:14-58:7; Vol. 4, p. 36:8-10; TR EX 27 (ICG Report); *see also* TR EX 351;
18 Menard Trial Designations, p. 62:11-15; TR EX 39 (Investigative Report); Ereiser
19 Trial Testimony 4/22/08, Vol. 2, pp. 58:5-13, 53:22-54:20.)

20 63. The only name Tarnovsky did not admit to in the ICG report is
21 “Nipper.” (Tarnovsky Trial Transcript 04/23/08, Vol. 2, p. 59:8-22.)

22 64. Tarnovsky admitted that the other information on the ICG report is
23 substantially correct, however. (*Id.*, p. 59:23-63:17; TR EX 27 (ICG Report).)

24 65. Moreover, the fundamental components and methodologies of NDS’s
25 hack (contained in the Headend Report) and the hack posted by “Nipper” on DR7
26 (the “Nipper Post”) are materially identical. (Avi Rubin Trial Testimony 4/16/08,
27 Vol. 3, p. 43:15-18.)

28 66. Both NDS’s hack and the Nipper Post contain the same fundamental

1 four fundamental components:

- 2 • they exploit a buffer overflow in the same way;
- 3 • they rely on the RAM ghosting or memory aliasing property unknown
- 4 to the general public;
- 5 • they rely on and demonstrate a complete understanding of the
- 6 operation of the index variable; and
- 7 • they use an incorrect checksum which causes a jump to the end of the
- 8 stack , where the shell code is located.

9 (Avi Rubin Trial Testimony 4/16/08, Vol. 3, p. 29:9-30:4; Mordinson Trial
10 Testimony 4/11/08, Vol. 2, p. 48:29-49:4-5.)

11 67. The Nipper Post could not have been done without access to the
12 Headend Report; while buffer overflow attacks are common, the method used in the
13 Headend Report and the Nipper Post is complicated and relies on things that were
14 not commonly known. (*Id.* p. 40:13-14; Vol. 4, p. 8:3-18.)

15 68. Additionally, Marco Pizzo ("Pizzo"), who used the alias "xbr21," saw
16 the full EchoStar code posted on a U.K. website on December 23, 2000. Pizzo cut
17 and pasted the code to DR7 a few hours later; and was certain no one could have
18 posted the EchoStar code to DR7 before he did. (Pizzo Trial Testimony 04/24/08,
19 Vol. 1, pp. 56:18-57:1, 58:15-59:9, 72:15-20, 75:4-12; TR EX 511-A (xbr21
20 reposting on dr7.com).)

21 69. Yet, Tarnovsky reported the posting of the EchoStar code on the
22 Internet to Defendants on December 22, 2000 when he sent an e-mail to NDS
23 employees entitled "Cat's Out of the Bag" (referring to the post of Plaintiffs' code
24 on DR7 - a day *before* Pizzo first saw the code on the Internet). (*See* TR EX 113;
25 Tarnovsky Trial Testimony 04/23/08, Vol. 4, p. 27:21-25.) Tarnovsky simply
26 could not have known about the DR7 posting on December 22 (which was no
27 longer posted by December 23) unless he had posted the code himself.

28 70. Finally, and poignantly, NDS was responsible for hacking the CAS of
Canal+, which was substantially similar to the EchoStar hack and which also was

1 posted on the Internet. (Saggiore Trial Testimony 4/16/08, Vol. 2, p. 50:25-52:15;
2 Mordinson Trial Testimony 04/11/08, Vol. 1, p. 35:25-36:14; Shkedy Trial
3 Testimony 04/10/08, Vol. 2, p. 49:11-18.)

4 71. At the time of the Nipper Post, Tarnovsky's salary was not paid by his
5 employer NDS Americas; rather, it was paid by a related entity, HarperCollins.
6 (Abe Peled Trial Testimony 05/6/08, Vol. 2, p. 104:1-3.)

7 72. Also, at the end of 2006, Mr. Tarnovsky received a \$5,000 bonus from
8 NDS Israel (also not Tarnovsky's employer) – home to the Haifa Research Center
9 from which the EchoStar hack originated. (*Id.*, p. 104:4-9.)

10 **Plaintiffs Were Materially Harmed by Defendants' Conduct.**

11 73. Defendants' hack methodology and the identified vulnerability, which
12 was published on the Internet in December 2000, was effective as to all EchoStar
13 ROM3 access cards and allowed pirates (and others) to make their own pirated
14 ROM3 cards. (Nicolas Trial Testimony 4/15/08, Vol. 1, p. 42:7-21.)

15 74. These pirated ROM3 cards then could be used to circumvent
16 Plaintiffs' security system and steal EchoStar's copyrighted programming. (*Id.* pp.
17 23:6-18, 23:19-24:1, 42:7-16.)

18 75. Immediately following the December 2000 postings, NagraCard's
19 Senior Vice President and Chief Technology Officer, Christophe Nicolas, led the
20 team that developed software updates (patches) and a February 2001 electronic
21 countermeasure ("ECM") designed to combat the piracy. (*Id.*, p. 68:21-71:15.)

22 76. Combating the piracy was not a simple matter, because any change to
23 the code could seriously slow the operation of the card and thus increase the wait
24 time of the customer using an EchoStar receiver. (Avi Rubin Trial Testimony
25 4/16/08, Vol. 3, p. 127:1-129:8.)

26 77. This is illustrated by the fact that when Nagra issued a patch or ECM
27 in February 2001, the programming had to be completely restructured. (*Id.*, p.
28 127:1-129:8.)

1 78. The ECM launched in February 2001 was designed to disable pirate
2 access cards that had been reprogrammed using Defendants’ hack methodology
3 published on the Internet. (Nicolas Trial Testimony 04/15/08, Vol. 1, p. 70:14-
4 71:15.)

5 79. But the patch was not completely effective, because pirates could
6 circumvent it with a blocker or by “glitching.” (Avi Rubin Trial Testimony
7 4/16/08, Vol. 3, p. 134:2-16; Vol. 4, p. 4:7-9; Nicolas Trial Testimony 04/15/08,
8 Vol. 1, p. 71:16-72:5; Tarnovsky Trial Testimony 04/23/08, Vol. 4, pp. 54:22-25,
9 55:7-10 (pirates used blockers to block the ECMs and glitching to “bounce over”
10 them).)

11 80. Nonetheless, Plaintiffs continued to try to combat piracy. Eventually,
12 however, a global card swap of all DNASP-II access cards with a different
13 encryption platform became necessary even though Plaintiffs did everything to
14 avoid a card swap. (Nicolas Trial Testimony 04/15/08, Vol. 1, p. 72:6-73:6; *see*
15 *also* Tarnovsky Trial Testimony 04/23/08, Vol. 3, p. 35:18-36:1; TR EX 41.)

16 81. The global card swap began in 2002 and ended in 2005. (Nicolas Trial
17 Testimony 04/15/08, Vol. 1, p. 72:6-72:23; Vol. 2, p. 77:2-8; *see also* Tarnovsky
18 Trial Testimony 04/23/08, Vol. 3, p. 35:18-36:1; TR EX 41.)

19 82. The cost to EchoStar of the global card swap were almost
20 \$94,638,625.10. (Lenoir Trial Testimony 04/10/08, Vol. 1, p. 64:11-16; Orban
21 Trial Testimony 04/17/08, Vol. 4, p. 8:7-13:2.) Thus, the value to EchoStar of a
22 secure card is approximately \$94, 638, 625.10.

23 83. The global card swap cost NagraStar approximately \$1.3 million.
24 (Lenoir Trial Testimony 04/10/08, Vol. 1, p. 64:11-16.)

25 84. NagraStar also suffered damages to its reputation and to its goodwill
26 with customers. (Lenoir Trial Testimony 04/10/08, Vol. 1, p. 64:21-65:8.)

27 85. The costs of piracy are ultimately borne by the consumer; if piracy is
28 significant, it results in an increase in security costs, which are then passed on to the

1 consumer through increases in pricing. (Peled Trial Testimony 5/6/08, Vol. 2, pp.
2 117:9-21, 118:9-13.)

3 **II. DISCUSSION AND CONCLUSIONS OF LAW**

4 **A. Defendants Have Engaged in Unlawful Business Practices.**

5 California Business and Professions Code § 17200 includes in its definition
6 of unfair competition any unlawful business practice – *i.e.*, a business practice that
7 violates another law. Any act that is forbidden by law, either civil or criminal;
8 federal, state, or municipal; statutory, regulatory, or court-made can be a predicate
9 for § 17200 liability. *People v. Fremont Life Ins. Co.*, 104 Cal. App. 4th 508, 515
10 (2003); *Nat’l Rural Telecom. Coop. v. DirecTV, Inc.*, 319 F. Supp. 2d 1059, 1074
11 (C.D. Cal. 2003). In effect, the “unlawful” prong of § 17200 makes a violation of
12 the underlying law a *per se* violation of § 17200. *Kasky v. Nike, Inc.*, 27 Cal. 4th
13 939, 950 (2002); *Cel-Tech Communications, Inc. v. Los Angeles Cellular Tele. Co.*,
14 20 Cal. 4th 163, 180 (1999); *Farmers Ins. Exch. v. Superior Court*, 2 Cal. 4th 377,
15 383 (1992). Moreover, California Business and Professions Code remedies and
16 penalties are cumulative to those imposed under other laws. *Id.*

17 A violation of any statute or regulation can be a predicate for § 17200
18 liability. In *Southwest Marine, Inc. v. Triple A Machine Shop, Inc.*, 720 F. Supp.
19 805 (N.D. Cal. 1989), the plaintiff, an unsuccessful bidder on a Navy contract, sued
20 the successful bidder, alleging that the successful bidder was able to underbid only
21 because of its practice of illegally disposing of hazardous wastes, allowing its costs
22 to be lower than those of the unsuccessful bidder plaintiff. 720 F. Supp. at 807.
23 The successful bidder’s disposing of hazardous wastes was alleged to be a violation
24 of several environmental laws, as well as a Navy procurement regulation that
25 required bidders to certify their compliance with all existing laws. *Id.* The Court
26 held that these allegations stated a claim for relief under § 17200. *Id.* at 808; *see*
27 *also Citizens for a Better Environment-California v. Union Oil of Cal.*, 996 F.
28 Supp. 934, 938 (N.D. Cal. 1997) (holding liability under § 17200 could be

1 predicated on a violation of the Federal Clean Water Act).

2 Similarly, in *People v. E.W.A.P. Inc.*, 106 Cal. App. 3d 315, 317 (1980), the
3 Court found that an unlawful business practice was adequately pled where the
4 defendant was alleged to have distributed obscene matter in violation of California
5 Penal Code § 311.2. 106 Cal. App. 3d at 317. The Court observed that “[Section
6 17200] [is] liberally construed so as not to be limited to traditional anticompetitive
7 practices.” *Id.* at 318. The Court further noted that the California Supreme Court
8 has stated that the meaning of unfair competition is “anything that can properly be
9 called a business practice and that at the same time is forbidden by law.” *Id.* at 319
10 (quoting *Barquis v. Merchants Collection Assn.*, 7 Cal. 3d 94, 112-113 (1972)).

11 A single act is sufficient to constitute a “business practice” under § 17200; it
12 does not require proof of a pattern or course of conduct. *Klein v. Earth Elements,*
13 *Inc.*, 59 Cal. App. 4th 965, 969 n.3 (1997); *Podolsky v. First Healthcare Corp.*, 50
14 Cal. App. 4th 632, 653-54 (1996).

15 Here, the jury found that Defendants have violated the Communications Act
16 of 1934, 47 U.S.C. § 605(a) and California Penal Code § 593e(b), all to gain a
17 competitive advantage over Plaintiffs. While the Court must make its own
18 independent findings, it may adopt the jury’s findings as appropriate. *A-C Co. v.*
19 *Security Pacific Nat. Bank*, 173 Cal.App.3d 462, 474, 219 Cal.Rptr. 62, 69 (Dist. 4
20 1986).

21 Therefore, the Court makes the following conclusions of law:

22 1. The jury’s finding that Defendants violated the Communications Act
23 of 1934, 47 U.S.C. § 605(a) and California Penal Code §§ 593d(a) and 593e(b) is
24 supported by the evidence, therefore the Court adopts the jury’s finding.

25 2. Because a violation of any *one* of these statutes is a *per se* violation of
26 § 17200, Defendants have engaged in an unlawful business practice in violation of
27 § 17200.

1 **B. Defendants Have Engaged In Unfair Business Practices.**

2 Even absent a statutory violation by Defendants, Plaintiff may recover under
3 the “unfair” prong of § 17200. Indeed, because the purpose of the antitrust law is to
4 encourage competition by prohibiting “practices by which fair and honest
5 competition is destroyed or prevented,” conduct may be unfair under § 17200 even
6 if it is not specifically proscribed by some other law. *Cel-Tech Comm., Inc.*, 20
7 Cal. 4th at 186 (quoting Cal. Bus. & Prof. Code § 17001).

8 In *Cel-Tech*, the California Supreme Court articulated a test for determining
9 when a business practice constitutes unfair competition. *Id.* at 186-87. A
10 competitor’s act or practice is “unfair” if it: (1) threatens an incipient violation of an
11 antitrust law, (2) violates the policy or spirit of one of those laws because its effects
12 are comparable to or the same as a violation of the law, or (3) otherwise
13 significantly threatens or harms competition. *Id.* The plaintiffs alleged that the
14 defendants, a cellular phone service and sales duopoly, sold phones at below market
15 prices subsidized by service revenues. *Id.* at 168-69. Several companies that
16 competed with the service-provider defendants challenged these practices as unfair
17 competition under § 17200. *Id.* The California Supreme Court found that the
18 plaintiffs had alleged plausibly anti-competitive conduct, even though the conduct
19 may not have risen to the level of a violation of antitrust law. *Id.* at 188-91.

20 Similarly, in *MGA Entertainment, Inc. v. Mattel Inc.*, Judge Manella stated
21 that “the purpose of destroying a competitor by means that are not within the area
22 of fair and honest competition is a purpose that clearly subverts the goal of the
23 [antitrust laws].” *Mattel*, No. CV 05-2727 NM (RNBx), 2005 WL 5894689 (C.D.
24 Cal. Aug. 26, 2005) (unpublished) (quoting *Northeast Airlines, Inc. v. World*
25 *Airways, Inc.*, 262 F. Supp. 316, 319 (D. Mass. 1966)). Applying this principle, the
26 Court found that allegations by some of Mattel’s competitors, including that Mattel
27 competed by unfairly using its extraordinary market power to preclude other
28

1 companies and brands from entering and competing in the market, rather than by
2 creating a better product or lowering its prices, were sufficient to state a claim
3 under § 17200. *Mattel* at **8-9. Specifically, the plaintiff alleged that Mattel, in
4 response to a dwindling market share, engaged in serial copycatting of the
5 plaintiff's products and attempted to intimidate former employees and distributors
6 and retailers into terminating their relationships with plaintiff. *Id.* at **1-2. The
7 court held that such conduct, if proven at trial, supported a finding that Mattel's
8 practices were "unfair" under either the second or third prong of the *Cel-Tech* test
9 because the conduct violated the policy or spirit of, or had effects comparable to, a
10 violation of the antitrust laws, or because they otherwise significantly threatened or
11 harmed competition. *Id.* at *7.

12 In *Silicon Image, Inc. v. Analogix Semiconductor, Inc.*, Judge Spero in the
13 Northern District of California held that the plaintiff alleged unfair business
14 practices under § 17200 where the defendant competitor copied, without
15 authorization, the plaintiff's semiconductor design and configuration software and
16 marketed them as replacements for the plaintiff's product. No. C-07-0635 JCS,
17 2007 WL 1455903 at *6 (N.D. Cal. May 16, 2007) (unpublished). The plaintiff
18 enjoyed a competitive advantage in the marketplace, in part as a result of its
19 semiconductor designs, which it had developed "[a]t great expense and effort" and
20 which accounted for the "high performance" of its chips. *Id.* at *1. The defendant
21 undercut the plaintiff's efforts by copying the plaintiff's design and marketing its
22 chips as "drop-in replaceable" with the plaintiff's chips, even though use of the
23 defendant's chips with the plaintiff's configuration software violated the plaintiff's
24 Software License Agreement with its customers. *Id.* The court held that these
25 allegations could support the inference that the defendant's conduct, which created
26 a disincentive for semiconductor manufacturers to invest in the development of
27 semiconductor chips and related software, threatened to harm competition and thus
28 violated § 17200.

1 In this case, Defendants experienced a vulnerability in their CAS and feared
2 a resulting decline in their market share. Findings of Fact ¶¶ 14-15. Rather than
3 simply improve their product, they engaged in unfair, anticompetitive behavior
4 intended to hobble Plaintiffs' ability to compete in the marketplace. Defendants
5 hacked Plaintiffs' CAS, developed by Plaintiffs at great expense and effort.
6 Findings of Fact ¶ 6, 29-33. Defendants created a hack methodology and shared
7 this methodology with known satellite pirates. The hack methodology was then
8 published online, all for the purpose of gaining an unfair competitive advantage.
9 Findings of Fact ¶¶ 19-72. Because the costs of such piracy are ultimately passed
10 on to the consumer, in destabilizing Plaintiffs' CAS and forcing Plaintiffs to invest
11 in costly electronic countermeasures, patches, and eventually a global card swap,
12 Defendants created an environment that made it more difficult for Plaintiffs to
13 compete. Findings of Fact ¶¶ 73-85.

14 Therefore, the Court makes the following conclusion of law:

15 3. By developing a hack methodology and sharing with known satellite
16 pirates this methodology, which was published online to the general public, all for
17 the purpose of gaining an unfair competitive advantage, Defendants engaged in an
18 unfair business practice in violation of § 17200.

19 **C. Plaintiffs Are Entitled To Restitution And An Injunction.**

20 California Business and Professions Code § 17203 authorizes courts to make
21 [S]uch orders or judgments as may be necessary . . . to prevent the use
22 or employment by any person of any practice which constitutes unfair
23 competition, as defined in this chapter, or as may be necessary to
24 restore to any person . . . any money or property, which may have
been acquired by means of such unfair competition.

25 Cal. Bus. & Prof. Code § 17203. This includes restitution and injunctions. *Id.*
26 Restitution is cumulative to other remedies under either § 17200 itself or other
27 laws. *United States v. Traylor*, 978 F.2d 1131, 1132 (9th Cir. 1992) (affirming civil
28

1 penalties, criminal fines, and restitution); *People v. Toomey*, 157 Cal. App. 3d 1,
2 22-26 (1985) (affirming civil penalties and restitution).

3 The purpose of the restitution under § 17203 is to return to the victim the
4 value of the money or property taken from the plaintiff or obtained by the defendant
5 through an unfair business practice, and to penalize a defendant for past unlawful
6 conduct and thereby deter future violations. *People v. Beaumont Inv., Ltd.* 111 Cal.
7 App. 4th 102, 135, 3 Cal. Rptr. 3d 429, 455 (2003) (awarding tenant victims
8 restitution in the amount of rent monies that exceeded the ordinance maximum).
9 The concept is similar to restitution to victims of a crime pursuant to California
10 Penal Code § 1202.4(3)(a), which provides for mandatory restitution of the full or
11 partial value of stolen or damaged property. Cal. Pen. Code § 1202.4(3)(a).

12 Defendants here hacked Plaintiffs' SmartCard and splayed out its contents
13 for all the world to see and take advantage of. Findings of Fact ¶¶ 19-72. The
14 jury's verdict supports the Court's finding that the Defendants illegally
15 compromised Plaintiffs' CAS. Plaintiffs invested considerable sums in developing
16 and protecting their CAS and installing it in the homes of their customers. Findings
17 of Fact ¶ 82. Indeed, the development and installation of a secure card costs
18 Plaintiffs approximately \$94,638,625.10. *Id.* However, just as when a criminal
19 takes control of a victim's property and sells it, destroys it, or otherwise depletes its
20 value, the value of Plaintiffs' CAS was taken from them through Defendants' unfair
21 and unlawful business practices. *See People v. Baker*, 126 Cal. App. 4th 463 (Cal.
22 App. 5th Dist. 2005) (defendant required to pay restitution under the California
23 Penal Code to victims of cattle theft even though the cattle was returned because
24 the cattle had diminished in value). Accordingly, Plaintiffs seek restitution of the
25 value of Plaintiffs' CAS at the time it was rendered ineffective by Defendants.

26 Restitution under § 17203 requires only that Plaintiffs have been harmed – it
27 does not require a showing of damages. *People v. Toomey*, 157 Cal. App. 3d 1, 26,
28 203 Cal. Rptr. 642, 658 (1984). Indeed, because restitution is not intended to

1 benefit Plaintiffs by the return of money, but instead is designed to penalize a
2 defendant for past unlawful conduct and thereby deter future violations, the Court
3 may award restitution even in the absence of Plaintiffs' actual damages. *Id.* The
4 Jury's finding concerning Plaintiffs' actual damages thus not preclude this Court's
5 awarding Plaintiffs' restitution damages: the actual damages the Jury considered
6 were intended to "fully and fairly compensate the Plaintiffs" and were not intended
7 to penalize Defendants' conduct and deter future violations, as is the purpose of
8 restitution damages. *Compare* Jury Instruction, "Claim 3 Communications Act - 47
9 U.S.C. § 605(a) – Actual Damages," with *Toomey*, 157 Cal. App. 3d at 26.

10 Section 17203 also authorizes injunctive relief to enjoin anticompetitive
11 behavior. Courts have broad power to fashion an injunctive remedy consistent with
12 the Legislature's intent to permit courts to "enjoin ongoing wrongful business
13 conduct in whatever context such activity might occur." *Barquis v. Merchants*
14 *Collection Ass'n*, 7 C.3d 94, 111, 101 C.R. 745, 757 (1972). The Court may grant
15 an injunction enjoining anticompetitive conduct even where the defendant is not
16 currently engaged in the conduct, if Plaintiffs can demonstrate a reasonable
17 probability that the anticompetitive behavior will recur. *E.W.A.P. Inc.*, 106 Cal.
18 App. 3d at 315, 165 Cal. Rptr. at 73 (illegal conduct can be enjoined under § 17200
19 if it is a business practice).

20 Plaintiffs have established that through a scheme that spanned more than
21 three years, Defendants developed a methodology to hack Plaintiffs' CAS, which
22 was posted on the Internet, enabling anyone to create a pirated SmartCard and steal
23 programming from Plaintiffs. Findings of Fact ¶¶ 19-72. Plaintiffs also established
24 that NDS hacked and facilitated the piracy of Canal+, and its own customer,
25 DirecTV. Findings of Fact ¶ 70. Given Defendants' prior conduct, there is a
26 reasonable probability that Defendants will engage in this or similar behavior in the
27 future. *Toomey*, 157 Cal. App. 3d at 1, 203 Cal. Rptr. at 642 (court found
28 likelihood that the defendant would repeat the offenses proper where defendant

1 continued to engage in other unfair business practices similar to the conduct that
2 formed the basis of the lawsuit).

3 Therefore the Court makes the following conclusions of law:

4 4. Plaintiffs have established that the value of the property taken from
5 them through Defendants' conduct (*i.e.*, a secure CAS) is \$94,638,625.10; Plaintiffs
6 therefore are entitled to restitution in this amount.

7 5. Because they engaged in a long term scheme to pirate Plaintiffs'
8 SmartCard, and hacked and facilitated the piracy of Canal+ and DirecTV, there is a
9 reasonable probability that Defendants will repeat their violations § 17200;
10 therefore, Plaintiffs are entitled to an injunction enjoining Defendants' unlawful
11 conduct.

12
13 DATED: June 5, 2008

14 Respectfully submitted,

15 **DLA PIPER US LLP**

16
17 By: /s/Cynthia A. Ricketts

18 Cynthia A. Ricketts

19 Attorneys for Plaintiffs

20 ECHOSTAR SATELLITE CORPORATION,

21 ECHOSTAR COMMUNICATIONS

22 CORPORATION, ECHOSTAR TECHNOLOGIES

23 CORPORATION, AND NAGRASTAR L.L.C.

24 Additional Counsel:

25 **T. WADE WELCH & ASSOCIATES**

26 T. Wade Welch (*pro hac vice*)

27 David M. Noll (*pro hac vice*)

28 2401 Fountainview, Suite 700

Houston, Texas 77057

Telephone: (713) 952-4334

Facsimile: (713) 952-4994

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

DLA PIPER US LLP
David A. Grenardo (State Bar No. 223142)
Cynthia A. Ricketts (*pro hac vice*)
1999 Avenue of the Stars, 4th Floor
Los Angeles, CA 90067
Telephone: (310) 595-3031
Facsimile: (310) 595-3331