

1 for: (a) the full dump of Plaintiffs' secret ROM Code; (b) the full dump of
 2 Plaintiffs' EEPROM Code and accompanying secret keys; and (c) the instructions
 3 on how to internally 'hack' or access Plaintiffs' microprocessor thereby granting
 4 the ability to 'read' and 'write' to Plaintiffs' Access Cards. In essence, Defendants'
 5 December 21, 2000 posting provided hackers for the first time with the 'Exploit
 6 key' or method necessary to gain access to Plaintiffs' microprocessor and
 7 subsequently read and write to Plaintiffs' Access Cards. The result of such dump
 8 also enabled a pirate/hacker to locate and identify Plaintiffs' secret "box keys" and
 9 secret "decrypt keys."

10 106. On December 24, 2000, Tarnovsky used the alias "NiPpEr2000" to
 11 publish the FULL Echo ROM Code, which had been modified to create a 3M
 12 counterfeit EchoStar access card, on www.piratesden.com. "NiPpEr2000's" post,
 13 entitled "tHe ReAl V3 DuMp!," states: "tHeRe WiLL bE nO bOxEs aNyMoRe!
 14 tHeRe WiLL bE nO mOrE fIgHtInG aMoNgSt uS. LeArN fRoM ThIs aNd
 15 pRosPer. tHiS WiLL Be PoStEd To ALL NeWsGrOuPs ArOuNd ThE WoRlD!
 16 ThIs Is Dr7'S cOdE (WeSt 3M v3) tHe rEaL sTuFf!!" Tarnovsky then goes on
 17 to state: "I wILL dUmP ALL vErSiOnS oF tHe WeSt CoDe LoOk FoR iT hErE!
 18 nIpPeR cLaUz 00" .

19 107. The first harmful effect of Tarnovsky providing this information was
 20 that every ROM3 EchoStar Access Card (approximately 7.6 million in circulation
 21 at that time) could then be compromised and forced to dump the EEPROM Code
 22 segment revealing the location and identity of Plaintiffs' secret "pairing keys." As
 23 a result, a pirate/hacker was now able to personally update a Pirated EchoStar
 24 Access Card or other Circumvention or Signal Theft Device to comport with
 25 Plaintiffs' frequent "pairing key" changes. Before December, 2000, a pirate/hacker
 26 was dependent on NDS, Tarnovsky and/or Menard, to either (1) have Nipper
 27 [Tarnovsky] provide the new "pairing keys" on pirate websites; or (2) send the
 28 disabled Pirated EchoStar Access Card back to the dealers for updating. However,

1 as a result of Tarnovsky's publications in December 2000, hackers around the
2 world now had the information necessary to personally circumvent any future
3 EchoStar pairing key change to a ROM3 Access Card. Users now simply inserted
4 the disabled Access Card into a card reader, performed the sequence of commands
5 and data provided by Tarnovsky which would identify the new pairing key change,
6 and update the Access Card with the new pairing keys. After performing these
7 steps, the user's Pirated EchoStar Access Card or other signal theft device was no
8 longer disabled and could once again receive unauthorized access to EchoStar
9 Programming.

10 108. Shortly after Defendants' December 2000 publications, the first
11 harmful effect evolved into the outright destruction and full compromise of
12 Plaintiffs' Security System. Given the information Tarnovsky provided, "Johnny
13 ASIC" was able to create and publish a modified version of Tarnovsky's
14 information consisting of another sequence of events and data that a pirate/hacker
15 could use to dump the entire ROM Code segment. The result of such dump enabled
16 the person to possess the intimate personal knowledge of how Plaintiffs' Security
17 System works. As a result of Tarnovsky's December 2000 publications, the piracy
18 world was now able to gain access, retrieve, and steal the heart and soul of
19 Plaintiffs' Security System and to dump both the EEPROM Code segment and the
20 requisite Nagra ROM Code segment.

21 109. Subsequent to these December 2000 postings, NDS, by and through
22 Tarnovsky, continued to provide technical information, support services, and
23 assistance related to EchoStar Access Cards and Plaintiffs' Security System, and
24 the unlawful circumvention and compromise thereof, to Menard and the "dealers"
25 of the NDS/Tarnovsky/Menard distribution network until the date that each such
26 dealer's unlawful website was shut down.

27 110. As a result of this information, support, and assistance, Menard and the
28 "dealers" of the NDS/Tarnovsky/Menard distribution network continued to: (a)

1 unlawfully reprogram EchoStar Access Cards; (b) unlawfully traffic in the sale
2 and/or distribution of reprogrammed EchoStar Access Cards; (c) periodically
3 update reprogrammed EchoStar Access Cards after they had been disabled and
4 rendered inoperable through one of Plaintiffs' ECMs; and (d) otherwise post or
5 provide technical information, support services, and assistance related to EchoStar
6 Access Cards and Plaintiffs' Security System by and through their websites to
7 facilitate others in the unlawful piracy and circumvention of Plaintiffs' CAS. This
8 unlawful conduct continued up to and including the following dates on which the
9 respective pirating websites were shut down: (1) January 28, 2001 – Sergei –
10 www.koinvizion.com; (2) June 21, 2001 – Menard – www.dr7.com; (3) June 19,
11 2003 – Dawson – www.dsscanada.com; (5) June 19, 2003 – Quinn –
12 www.hitecsat.com; and (6) June 25, 2003 – Frost – www.newfrontiergroup.com.

13 111. NDS's wrongful conduct also gave other satellite pirates the ability to
14 design, manufacture, sell, or otherwise traffic in Pirated EchoStar Access Cards and
15 other Circumvention or Signal Theft Devices for a profit and the ability to release
16 Plaintiffs' proprietary information to other satellite pirates for the same or similar
17 purpose.

18 112. Specifically, on or about May 31, 2001, a Pirates Den "DISH
19 Network" file search yielded the following downloadable illegal files related to
20 circumvention of Plaintiffs' Security System in order to receive the unauthorized
21 viewing of DISH Network programming services: (1) sorry Charlie 2.8 (sc28.exe);
22 (2) 2 Piece AVR (2pieceavr.zip); (3) msg306src (mcg306src.zip); (4) EEEdit
23 (eepedit.zip); (5) Mracttv2 (mracttv2.zip); (6) Nagra Blocker
24 (nagra_blocker21.zip); (7) Rom2 Disassembly (rom2.zip); (8) Talk10 (talk10.zip);
25 (9) Dish500 (dish500.zip); (10) Edit305 (edit305v1.zip); (11) Virgin Bin
26 (virgin.zip); (12) Stuntguy's NagraVision hacking FAQ (erom_faq_012000.zip);
27 (13) E3m Disassembly (e3ms.zip); (14) 288-02 disassembly (disasm.zip); (15)
28 Simple ATME: Programmer \$5 in parts (13418eprog.zip); (16) Wbininfo150

1 (wbininfo150.zip); (17) Dish 3m (dish3m.zip); (18) Sorry Charlie
2 (sorrycharlie.zip); (19) Talk 31d (talk31d.zip); (20) 01-02 Dumps (0102dumps.zip);
3 (21) Talk3.1b (talk31b.zip); (22) Fbprg16 (fbprg.zip); (24) Dish Blank Bin
4 (dishblank.zip); (25) Dish PPV Wipe (dishppvwiipe.zip); (26) EDump (edump.zip);
5 (27) Dish Hardware FAQ (faqdishhdwr.zip); (28) MCG305 (mcg305.zip); (29)
6 **E3m code (west3mv3.zip)**; and (30) Talk 3.1 (talk31.zip).

7 113. On or about December 16, 2001, Tarnovsky admits to Giles Kaehlin,
8 Head of Security for Canal+, at a meeting in London, that NDS was responsible for
9 the hack and publication of the DISH Network ROM Code on the internet.
10 Tarnovsky admits that the DISH Network code was sent to him by Reuven Hasak,
11 head of security for NDS in Israel, from John Norris, head of security for NDS
12 Americas. Tarnovsky later sent an email stating that he wanted no further
13 communications to occur between himself and Kaehlin.

14 114. As a result of Tarnovsky's conduct outlined above, he became the
15 target of an investigation by the federal government. Specifically, various packages
16 containing up to \$20,100.00 in cash hidden in various electronic devices were
17 intercepted in transit from Menard to Tarnovsky. Plaintiffs are informed and
18 believe that said payments, which were being sent daily from Menard to Tarnovsky,
19 with the assistance of Main, constituted compensation for Tarnovsky reactivating
20 the reprogrammer such that Menard could produce more unlawfully altered
21 EchoStar Access Cards using NDS and Tarnovsky's "stinger."

22 115. On or about December 14, 2000, U.S. Customs advised the Hays
23 County Narcotics Task Force that *Tarnovsky worked for NDS in California and was*
24 *believed to be counterfeiting or pirating satellite T.V. access cards.* U.S. Customs
25 was working with Direct TV's private security company who was also investigating
26 Tarnovsky's hacking activities. Plaintiffs are informed and believe that U.S.
27 Customs also investigated Tarnovsky on a case in the states of Oregon and
28 Washington.

1 116. On or about January 9, 2001, a “knock and talk” by U.S. Customs
2 agents Flannigan and Spears, as well as Ruben Romero of Galaxy Latin America,
3 takes place at Tarnovsky’s house in California. During the walkthrough, Agents
4 witnessed various electronic equipment believed to be used for reprogramming
5 EchoStar access cards.

6 117. On or about March 8, 2001, at a meeting with Menard in Canada with
7 Ereiser present, *Menard stated that “Tarnovsky would lose his job”* if Menard
8 provided any information as to how the initial hack of Plaintiffs’ conditional access
9 system occurred. Tarnovsky was an employee and agent of NDS at this time.

10
11 **VII. PLAINTIFFS HAVE BEEN, AND CONTINUE TO BE,**
12 **SUBSTANTIALLY INJURED BY DEFENDANTS’ ILLEGAL**
13 **CONDUCT**

14 118. Since NDS’s hacking EchoStar’s Access Card and posting its hack
15 methodology on the Internet in December 2000, Pirated EchoStar Access Cards and
16 other Circumvention or Signal Theft Devices have become available. Plaintiffs
17 have also been and continue to be substantially injured as a result of the
18 proliferation of their Security System effectuated by Tarnovsky and Menard
19 reprogramming cards, distributing same through Dawson, Quinn, Sergei and Frost,
20 and subsequently providing technical support for same. These unlawful acts
21 continued up to and including June 25, 2003 when the last distributor’s website was
22 shut down.

23 119. These Pirated EchoStar Access Cards and other Circumvention or
24 Signal Theft Devices enable, assist, and facilitate the decryption of DISH
25 Network’s Programming services without EchoStar’s authorization or viewers’
26 payment of the necessary and required fees. These Pirated EchoStar Access Cards
27 and other Circumvention or Signal Theft Devices have been, and continue to be,
28 advertised, marketed, distributed, and sold via the Internet, local publications, and

1 in underground satellite publications, in addition to being often times sold by
2 satellite equipment retail dealers. Regardless of how these Pirated EchoStar Access
3 Cards and other Circumvention or Signal Theft Devices are advertised, marketed,
4 distributed, or sold, the fact of the matter is that these Pirated EchoStar Access
5 Cards and other Circumvention or Signal Theft Devices would not presently exist
6 but for the wrongful conduct of Defendants, as described herein.

7 120. Defendants' wrongful conduct has injured, and will continue to injure,
8 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
9 other valuable consideration, compromising Plaintiffs' conditional access system,
10 infringing on Plaintiffs' trade secrets and proprietary information, and interfering
11 with Plaintiffs' contractual and prospective business relations. And, as a direct
12 result of Defendants' December 2000 postings, Plaintiffs were forced to employ
13 their very first card swap of approximately more than 7 million EchoStar Access
14 Cards.

15
16 **VIII. PLAINTIFFS' MOTION TO INTERVENE IN THE CANAL+ V. NDS**
17 **LITIGATION**

18 121. Hacking Plaintiffs' Security System is not the first time NDS has
19 engaged in wrongful behavior against a competitor's Security System. On or about
20 April 9, 2002, Oliver Kommerling, NDS's employee and agent, explained the
21 methods that NDS used to break the Security System of another encryption
22 competitor, Canal+, and to distribute that information to foster satellite piracy.

23 122. Kommerling testified that "NDS engineers in the NDS facility in
24 Haifa, Israel obtained Canal+ Access Cards and using the techniques taught by me
25 [Kommerling] (some of which were described in my paper Design Principles for
26 Tamper Resistant Smartcards written with Markus Kuhn) were able to physically
27 extract the Canal+ machine code embedded in their Access Cards." Further
28 Kommerling testified that "NDS engineers disassembled and analyzed the extracted

1 machine code . . .” which was later confirmed by Kommerling as the same code
2 that was published on the “DR7 website” by NDS agent Christopher Tarnovsky.
3 (Kommerling Dec. ¶ 6(a)-(e), attached hereto.)

4 123. Upon further investigation, in approximately early September 2002,
5 Plaintiffs discovered the sworn declaration of Jan Saggiori, an employee of SSS
6 LLC, based in Geneva Switzerland. Saggiori testified that he “asked Chris
7 Tarnovsky if he could obtain the [missing] code present at the 2000 address from
8 Al Menart. By an email exchange from Chris Tarnovsky [on March 28, 1999],
9 Chris sent me [Saggiori] an 8kb binary file that he claimed contained the requested
10 code extracted from the Canal+ smart card.” (Saggiori Dec. ¶ 5 and Exhibits to his
11 declaration, attached hereto)

12 124. Upon Plaintiffs’ receipt and review of the code sent from NDS
13 employee Tarnovsky to Saggiori, Plaintiffs discovered that the code was actually
14 from an ST microchip that NagraStar used within its Access Cards. As evidenced
15 by this code, and the well pleaded facts herein, Plaintiffs are now informed and
16 believe that NDS may have cracked Plaintiffs’ Security System as early as March
17 28, 1999 and distributed Plaintiffs’ illegally obtained proprietary codes at this time
18 through its employee and agent Tarnovsky, among other Defendants, with the
19 intent and common plan to facilitate the piracy of Plaintiffs’ Security System and
20 cause harm to Plaintiffs.

21 125. Upon discovering that NDS was responsible for the acts complained of
22 herein in approximately early September 2002, Plaintiffs immediately brought an
23 action against NDS on September 27, 2002 by filing a Motion to Intervene in
24 Canal+’s pending lawsuit against NDS – which was based upon similar facts and
25 circumstances. The *Canal+ v. NDS et al.* case settled before Plaintiffs’ Motion to
26 Intervene could be granted. Accordingly, Plaintiffs filed this suit on June 6, 2003.

27
28 **IX. OUTLINE OF WRONGFUL CONDUCT AND THEORIES OF**

1 **LIABILITY UNDERLYING PLAINTIFFS' CLAIMS**

2 **A. NDS Group**

3 126. NDS Group used its laboratory in Haifa, Israel and its employees
4 (including Oliver Kommerling) to unlawfully obtain EchoStar Access Cards for the
5 purpose of hacking into Plaintiffs' microprocessor embedded in EchoStar Access
6 Cards to gain access to and extract therefrom Plaintiffs' proprietary and secret
7 ROM and EEPROM Codes secured therein. NDS Group also used the information
8 they extracted from EchoStar's access cards to develop a hack methodology which
9 would defeat EchoStar's security measures. (*See* 5AC ¶¶ 13, 82, 83; *see also*
10 Kommerling Decl. ¶ 7, Stewart Aff. ¶¶ 16, 20, 21, 26.)

11 127. Hasak subsequently transferred Plaintiffs' ROM and EEPROM Codes
12 from Israel to NDS Americas (Norris and Tarnovsky) with instructions for
13 Tarnovsky to use the codes to develop an unlawful reprogramming device to
14 modify Plaintiffs' Access Cards and create a distribution network to sell and
15 distribute the reprogrammed cards. (5AC ¶¶ 14-16, 84, 85, 109, 110; *see also*
16 Kommerling Decl. ¶ 7, Stewart Aff. ¶¶ 16, 20, 21, 26.)

17 128. As a result of the foregoing, NDS Group is directly and secondarily
18 liable for the unlawful acts of piracy committed by: (a) NDS Americas and its
19 employees (Norris and Tarnovsky), (*See* 5AC ¶¶ 38; *see also* Kommerling Decl. ¶
20 7, Stewart Aff. ¶¶ 26); (b) NDS Americas agent Menard, (*See* 5AC ¶¶ 40, 41); (c)
21 NDS Americas' sub-agent "dealers" in the NDS/Tarnovsky/Menard distribution
22 network (Dawson, Quinn, Sergei, and Frost), (*See* 5AC ¶¶ 42, 43); and (d) all end-
23 user satellite pirates who received reprogrammed EchoStar Access Cards or
24 subsequent technical support for same from any of the foregoing Defendants in
25 furtherance of Hasak's directives to Tarnovsky and Norris. (*See* 5AC ¶¶ 118, 119).
26 Specifically, NDS Group and its employees are secondarily liable under the
27 following theories: (1) aiding and abetting, (*See* 5AC ¶¶ 16, 17, 89, 90, 92); (2)
28

1 contributory and/or vicarious copyright infringement, (*See* 5AC ¶¶ 118, 119); and
2 (3) conspiracy/joint contribution (*See* 5AC ¶¶ 46-48). NDS Group's secondary
3 liability for the unlawful acts committed by any of the foregoing Defendants under
4 the foregoing theories continued up to and including June 25, 2003 – the date the
5 last website through which the NDS/Tarnovsky/Menard distribution network
6 operated was shut down. (*See* 5AC ¶¶ 24, 25, 95, 110).

7
8 **B. NDS Americas**

9 129. NDS Americas, by and through Norris and Tarnovsky, received
10 Plaintiffs' proprietary and secret ROM and EEPROM Codes that were unlawfully
11 obtained and extracted by NDS Group through Norris and Tarnovsky via Hasak,
12 (*See* 5AC ¶¶ 13, 14, 84; *see also* Stewart Aff. at ¶ 26).

13 130. NDS Americas, by and through Norris and Tarnovsky, used Plaintiffs'
14 Codes to design and build an unlawful reprogramming device capable of modifying
15 EchoStar Access Cards. (*See* 5AC ¶¶ 15, 84, 85, 87).

16 131. NDS Americas, by and through Norris, instructed Tarnovsky to set up
17 a distribution network through which the unlawfully reprogrammed EchoStar
18 Access Cards could be marketed, sold, and distributed to the pirating public. (*See*
19 5AC ¶¶ 16, 17, 89, 90; *see also* Scullion Decl. at ¶ 12, 17).

20 132. Under this directive, Tarnovsky successfully solicited Menard to: (a)
21 use the NDS reprogrammer to reprogram EchoStar Access Cards, (*See* 5AC ¶¶ 16,
22 17, 87, 88); (b) assist in establishing and maintaining a distribution network through
23 which these cards could be marketed, sold, and distributed, (*See* 5AC ¶¶ 89-97);
24 and (c) assist Tarnovsky in the posting of software, instructions, codes, fixes,
25 updates and/or other technical support for the reprogrammed EchoStar Access
26 Cards, (*See* 5AC ¶¶ 94; *see also* Scullion Decl. at ¶¶ 12, 17).

27 133. With the assistance and protection of NDS Americas, by and through
28 Norris and Tarnovsky, Menard successfully solicited Dawson, Quinn, Sergei and

1 Frost to serve as distributors of the reprogrammed EchoStar Access Cards and
2 software and technical support for same and to assist in the maintenance of the
3 distribution network. Menard also successfully solicited the assistance of Main, as
4 a “courier” to traffick in same. (See 5AC ¶¶ 16, 17, 44; *see also* Scullion Decl. at ¶
5 18).

6 134. Through Tarnovsky and Norris, NDS controlled Menard and the
7 distribution network. (See 5AC ¶¶ 16, 18, 39-41, 90, 98, 99; *see also* Scullion Decl.
8 at ¶ 17-19).

9 135. Through Menard and the distributors (Dawson, Quinn, Sergei and
10 Frost), NDS Americas and Tarnovsky were able to unlawfully reprogram EchoStar
11 Access Cards, distribute these reprogrammed cards to pirating end-users, and
12 provide technical support for same with this conduct continuing up to and including
13 June 25, 2003 when the last NDS distribution website was shut down. (See 5AC ¶¶
14 16, 24, 25, 95, 110; *see also* Scullion Decl. at ¶ 17-19).

15 136. Tarnvosky continued in unlawfully reprogramming EchoStar Access
16 Cards directly up to and including January 9, 2001 when his home was visited by
17 federal officials in connection with a federal investigation into Tarnovsky’s
18 activities. (See 5AC ¶¶ 26, 116).

19 137. Under the instruction and direction from NDS Americas, on December
20 21 and 24, 2000, Tarnovsky caused Plaintiffs’ ROM and EEPROM codes extracted
21 from Plaintiffs’ microprocessor by NDS Group and all necessary instructions to
22 utilize same for reprogramming EchoStar Access Cards in the circumvention of
23 Plaintiffs’ CAS, to be posted on the Internet resulting in the immediate widespread
24 compromise of Plaintiffs’ Security System. (See 5AC ¶¶ 19-23, 103, 106).

25 138. In addition to NDS Americas and its employees (Norris and
26 Tarnovsky) direct liability for the foregoing acts, they are also secondarily liable
27 for: (a) the acts of each other; (b) NDS Americas agent Menard, (See 5AC ¶¶ 40,
28 41, 89, 90; *see also* Scullion Decl. at ¶ 12, 17); (c) NDS sub-agent distributors

1 Dawson, Quinn, Sergei, and Frost, (*See* 5AC ¶¶ 42, 43, 89-91; *see also* Scullion
2 Decl. at ¶¶ 18, 26); and (d) all end-user satellite pirates who received
3 reprogrammed EchoStar Access Cards or subsequent technical support for same
4 from the any of the foregoing Defendants in furtherance of Hasak's directives to
5 Tarnovsky and Norris. (*See* 5AC ¶¶ 118, 119). Specifically, NDS Americas and its
6 employees (Norris and Tarnovsky) are secondarily liable under the following
7 theories: (1) agency with Menard, (*See* 5AC ¶¶ 40, 41, 89, 90); (2) agency/sub-
8 agency with the distributors of the NDS/Tarnovsky/Menard distribution network
9 (Dawson, Quinn, Sergei and Frost), (*See* 5AC ¶¶ 42, 43, 89-91; *see also* Scullion
10 Decl. at ¶ 18); (3) contributory and vicarious copyright infringement by Menard,
11 (*See* 5AC ¶¶ 40, 41, 89, 90; *see also* Scullion Decl. at ¶ 18), and the distributors of
12 the NDS/Tarnovsky/Menard distribution network (Dawson, Quinn, Sergei and
13 Frost), (*See* 5AC ¶¶ 42, 43, 89-91; *see also* Scullion Decl. at ¶ 18), as well as the
14 pirating end-users purchasing the reprogrammed cards and/or receiving technical
15 support for same, (*see* 5AC ¶¶ 118, 119); (4) agency by ratification of the foregoing
16 acts engaged in by the distributors of the NDS/Tarnovsky/Menard distribution
17 network (Dawson, Quinn, Sergei and Frost) on NDS Americas' behalf, (*see* 5AC ¶
18 45); (5) aiding and abetting Menard, (*see* 5AC ¶¶ 16, 17, 89, 90, 92; *see also*
19 Scullion Decl. at ¶ 17), and the distributors of the NDS/Tarnovsky/Menard
20 distribution network (Dawson, Quinn, Sergei and Frost), (*See* 5AC ¶¶ 16, 17, 91,
21 93, 95-97; *see also* Scullion Decl. at ¶ 18); and (6) conspiracy. (*See* 5AC ¶¶ 46-
22 48). NDS Americas' secondary liability for the unlawful acts committed by any of
23 the foregoing Defendants under the foregoing theories continued up to and
24 including June 25, 2003 – the date the last website through which the
25 NDS/Tarnovsky/Menard distribution network operated was shut down. (*See* 5AC ¶
26 24, 25, 92-95, 110).

27 C. **Menard and the NDS Distributors Dawson, Quinn, Sergei and**
28 **Frost**

1 139. After NDS Americas successfully solicited Menard, by and through
2 Tarnovsky, Menard agreed to (and did) assist NDS Americas and Tarnovsky in
3 establishing and maintaining a distribution network. (*See* 5AC ¶¶ 16-18, 89, 90).

4 140. In furtherance of that directive, Menard assisted NDS, by and through
5 Tarnovsky, in successfully soliciting Dawson, Sergi, Quinn and Frost to serve as
6 NDS distributors for the reprogrammed EchoStar Access Cards. (*See* 5AC ¶¶ 16,
7 17, 90, 91; *see also* Scullion Decl. at ¶ 18).

8 141. Menard used the reprogrammer device NDS provided to him, by and
9 through Tarnovsky, to unlawfully reprogram EchoStar Access Cards. (*See* 5AC ¶¶
10 16, 18, 92, 93; *see also* Scullion Decl. at ¶ 18).

11 142. Menard supplied reprogrammed EchoStar Access Cards to the NDS
12 distributors of the NDS/Tarnovsky/Menard distribution network (Dawson, Quinn,
13 Sergei and Frost) to market, sell, distribute to the pirating public. (*Id.*)

14 143. Through the business names of “X-Factor Design, Inc.,” “Hi-Fi Audio
15 Exchange,” and “Regency Audio,” his hacker website (www.dr7.com), and the
16 NDS distributors’ hacker websites (www.discountsatellite.com,
17 www.dsscanada.com, www.hitecsat.com, www.koinvizion, and
18 www.newfrontiergroup.com), among other Internet websites, Menard assisted
19 Tarnovsky in the posting of “software,” “instructions,” “codes,” “fixes,” “updates,”
20 and/or other technical support for the reprogrammed EchoStar Access Cards. (*See*
21 5AC ¶¶ 24, 25, 93-95; *see also* Scullion Decl. at ¶ 12).

22 144. Menard continued reprogramming EchoStar Access Cards and
23 providing technical support services for same up to and including June 19, 2001 –
24 the date his hacker website, www.dr7.com, was shut down. (*See* 5AC ¶¶ 24, 25, 27,
25 95, 110; *see also* Scullion Decl. at ¶ 12).

26 145. Sergei continued to advertise, provide, and otherwise traffic in
27 unlawfully reprogrammed EchoStar Access Cards and/or other Signal Theft
28 Devices, as well as technical support for same, up to and including January 28,

1 2001 – the date his hacker website, www.koinvizion.com, was shut down. (*See*
2 5AC ¶¶ 24, 25, 27, 95, 110).

3 146. Dawson continued to advertise, provide and otherwise traffic in
4 unlawfully reprogrammed EchoStar Access Cards and/or other Circumvention
5 Signal Theft Devices, as well as technical support for same, up to and including
6 June 19, 2003 when his website, www.dsscanada.com, was shut down. (*Id.*).

7 147. Quinn continued to advertise, provide and otherwise traffic in
8 unlawfully reprogrammed EchoStar Access Cards and/or other Circumvention
9 Signal Theft Devices, as well as technical support for same, up to and including
10 June 19, 2003 when his website www.hitecsat.com was shut down. (*Id.*).

11 148. Frost continued to advertise, provide and otherwise traffic in
12 unlawfully reprogrammed EchoStar Access Cards and/or other Circumvention
13 Signal Theft Devices, as well as technical support for same, up to and including
14 June 25, 2003 when his website www.newfrontiergroup.com was shut down. (*Id.*).

15 D. **Main**

16 149. Main was successfully solicited by Menard to assist Menard in the
17 day-to-day maintenance of the NDS distribution network and Menard’s hacker
18 website which operated up to and including June 21, 2001 when it was shut down.
19 (*See* 5AC ¶ 24, 25, 27, 44, 95, 110.)

20
21 **X. CAUSES OF ACTION**

22 **FIRST CAUSE OF ACTION**

23 **(Circumventing Technological Measures Concerning Protected and**
24 **Copyrighted Works in Violation of the Digital Millennium Copyright Act, 17**
25 **U.S.C. § 1201(a)(1)(A))**

26 150. Plaintiffs hereby incorporate by reference 5AC ¶¶ 126-149, as if set
27 forth fully within this cause of action.

28 151. Defendants violated 17 U.S.C. § 1201(a)(1)(A) by directly or
indirectly circumventing Plaintiffs’ CAS that effectively control access to works

1 protected under Title 17 of the United States Code, namely DISH Network's
2 satellite television programming services and the protected works broadcasted
3 thereon.

4 Defendant NDS Group

5 152. Defendant NDS Group is directly and/or secondarily liable for the
6 unlawful circumvention activities committed by Defendants NDS Americas and its
7 employees (Norris and Tarnovsky), Menard, the "dealers" in the
8 NDS/Tarnovsky/Menard distribution network and other persons in violation of 17
9 U.S.C. § 1201(a)(1)(A) by engaging in the conduct stated in (5AC ¶¶ 12-27, 38-48,
10 82-85, 89-97, 101-106, 118, 119 & incorporated citations) under the theories
11 advanced therein, including but not limited to Tarnovsky's publication of the hack
12 methodology (which Defendants created) on pirate-websites on or about December
13 21 and 24, 2000.

14 Defendant NDS Americas

15 153. Defendant NDS Americas violated 17 U.S.C. § 1201(a)(1)(A) by and
16 through its employees (Norris and Tarnovsky) engaging directly in the conduct
17 stated in (5AC at ¶¶ 12-27, 38, 84-97, 101-106, & incorporated citations) under the
18 theories advanced therein, including but not limited to Tarnovsky's publication of
19 the hack methodology (which Defendants created) on pirate-websites on or about
20 December 21 and 24, 2000.

21 154. Defendant NDS Americas are also secondarily and/or contributorily
22 liable for the unlawful circumvention activities of Menard, the "dealers" in the
23 NDS/Tarnovsky/Menard distribution network, and other person committed in
24 violation of 17 U.S.C. § 1201(a)(1)(A) by engaging in the conduct stated in (5AC
25 ¶¶ 16-18, 39-48, 84-97, 118, 119 & incorporated citations) under the theories
26 advanced therein.

27 155. These acts complained of herein occurred in, amongst other places, the
28 State of California, Canada, and Israel.

1 156. Defendants' direct and indirect acts of circumvention were performed
2 without the permission, authorization, or consent of Plaintiffs or any owner of
3 copyrighted programming broadcasted on the DISH Network.

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

6 158. Pursuant to 17 U.S.C. § 1203, Plaintiffs are entitled to equitable relief,
7 damages (either statutory damages of \$200 to \$2,500 per violation, or actual
8 damages plus any profits realized by Defendants as a result of this unlawful
9 conduct), reasonable attorney's fees, and costs, in addition to all other relief to
10 which they may be entitled.

11 **SECOND CAUSE OF ACTION**

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

14 159. Plaintiffs hereby incorporate by reference 5AC ¶¶ 126-149, as if set
15 forth fully within this cause of action.

16 160. Defendants violated 17 U.S.C. §§ 1201(a)(2) by directly or indirectly
17 manufacturing, importing to the United States, offering to the public, providing or
18 otherwise trafficking in altered, modified, compromised and/or reprogrammed
19 EchoStar Access Cards or other Signal Theft Technology and Devices, including
20 but not limited to Defendants' December 2000 postings, knowing that such
21 technology or devices: (a) are primarily designed or produced for the purpose of
22 circumventing Plaintiffs' CAS or the protections afforded thereby to copyright
23 owners' rights of works or portions thereof; (b) have only limited commercially
24 significant purposes or uses other than to circumvent Plaintiffs' CAS or the
25 protections afforded thereby to copyright owners' rights of works or portions
26 thereof; or (c) were marketed by the following Defendants or another person acting
27 in concert with Defendants with Defendants' knowledge for use in circumventing
28 Plaintiffs' CAS or the protections afforded thereby to copyright owners' rights of

1 works or portions thereof.

2 Defendants NDS Group

3 161. Defendant NDS Group is secondarily liable for the unlawful activities
4 committed by Defendants NDS Americas and its employees (Norris and
5 Tarnovsky), Menard, the “dealers” in the NDS/Tarnovsky/Menard distribution
6 network and other persons in violation of 17 U.S.C. §§ 1201(a)(2) by engaging in
7 the conduct stated in (5AC ¶¶ 12-27, 38-48, 82-85, 89-97, 101-106 & incorporated
8 citations) under the theories advanced therein.

9 Defendant NDS Americas

10 162. Defendant NDS Americas violated 17 U.S.C. §§ 1201(a)(2) by
11 engaging in the conduct stated in (5AC at ¶¶ 12-27, 38, 84-97, 101-106 &
12 incorporated citations) under the theories advanced therein.

13 163. Defendant NDS Americas are also secondarily liable for the violations
14 of 17 U.S.C. §§ 1201(a)(2) of Menard, the “dealers” in the NDS/Tarnovsky/Menard
15 distribution network and other persons by engaging in the conduct stated in (5AC
16 ¶¶ 16-18, 39-48, 84-97, 118, 119 & incorporated citations) under the theories
17 advanced therein.

18 164. These acts complained of herein occurred in, amongst other places, the
19 State of California, Canada, and Israel.

20 165. Defendants’ violations have injured, and will continue to injure,
21 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
22 other valuable consideration, compromising Plaintiffs’ security and accounting
23 systems, infringing Plaintiffs’ trade secrets and proprietary information, and
24 interfering with Plaintiffs’ contractual and prospective business relations.

25 166. Defendants’ acts of circumvention were performed without the
26 permission, authorization, or consent of Plaintiffs or any owner of copyrighted
27 programming.
28

1 167. Defendants violated Sections 1201(a)(2) of the Digital Millennium
2 Copyright Act willfully, and for purposes of commercial advantage or private
3 financial gain.

4 168. Defendants knew that manufacturing, importing (to the United States),
5 offering to the public, providing, and trafficking in Pirated EchoStar Access Cards
6 and other Signal Theft Devices was and is illegal and prohibited.

7 169. Such violations have caused, and will continue to cause, Plaintiffs
8 irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such
9 continued violations. Unless restrained by this Court, Defendants will continue to
10 violate 17 U.S.C. § 1201(a)(2).

11 **THIRD CAUSE OF ACTION**

12 **(Facilitating the Unauthorized Reception of Satellite Signals in Violation of the**
13 **Communications Act of 1934, as amended, 47 U.S.C. § 605(a))**

14 170. Plaintiffs re-allege and incorporate 5AC ¶¶ 126-149, as if fully set
15 forth in this cause of action.

16 171. Defendants engaged in and/or assisted other persons in the
17 unauthorized reception of use of EchoStar's satellite transmissions of television
18 programming in violation of 47 U.S.C. § 605(a) by directly or indirectly designing,
19 manufacturing, developing, assembling, modifying, importing (to the United
20 States), distributing, selling, providing, or otherwise trafficking in reprogrammed
21 EchoStar Access Cards and other Signal Theft Technology and Devices, including
22 Defendants' December 2000 postings.

23 **Defendants NDS Group**

24 172. Defendants NDS Group are directly and/or secondarily liable for the
25 unlawful acts of Defendants NDS Americas, Menard, the "dealers" in the
26 NDS/Tarnovsky/Menard distribution network and other persons committed in
27 violation of 47 U.S.C. § 605(a) by engaging in the conduct stated in (5AC ¶¶ 12-27,
28

1 38-48, 82-85, 89-97, 101-106 & incorporated citations) under the theories advanced
2 therein.

3 Defendants NDS Americas

4 173. Defendants NDS Americas violated 47 U.S.C. § 605(a) by and through
5 its employees Norris and Tarnovsky engaging in the conduct stated in (5AC ¶¶ 16-
6 18, 39-48, 84-97, 118, 119 & incorporated citations) under the theories advanced
7 therein.

8 174. Defendants NDS Americas is secondarily liable for the unlawful acts
9 of Menard, the “dealers” in the NDS/Tarnovsky/Menard distribution network and
10 other persons committed in violation of 47 U.S.C. § 605(a) by engaging in the
11 conduct stated in (5AC at ¶¶ 12-27, 38, 84-97, 101-106 & incorporated citations)
12 under the theories advanced therein.

13 175. These acts complained of herein occurred in, amongst other places,
14 California, Canada, and Israel.

15 176. Defendants’ violations have injured, and will continue to injure,
16 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
17 other valuable consideration, compromising Plaintiffs’ security and accounting
18 systems, infringing Plaintiffs’ trade secrets and proprietary information, and
19 interfering with Plaintiffs’ contractual and prospective business relations.

20 177. Defendants’ acts of circumvention were performed without the
21 permission, authorization, or consent of Plaintiffs or any owner of copyrighted
22 programming.

23 178. Defendants violated Section 605(a) of the Communications Act
24 willfully, and for purposes of commercial advantage or private financial gain.

25 179. Defendants knew that assisting third persons in the reception and use
26 of EchoStar’s satellite transmissions of television programming, without
27 authorization, was and is illegal and prohibited.
28

1 180. Defendants' violations of 47 U.S.C. § 605(a) have injured, and will
2 continue to injure, EchoStar's ability to maximize the revenues which it seeks to
3 derive from its satellite television programming as EchoStar has been deprived of
4 the benefit of subscribers to EchoStar's satellite television programming.

5 181. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs are entitled to equitable
6 relief, damages (either statutory damages of \$1,000 to \$10,000 per violation, or
7 actual damages plus any profits realized by Defendants for each violation of 47
8 U.S.C. § 605(a)), and reasonable attorney's fees and costs. Plaintiffs seek all other
9 relief to which they may be entitled.

10
11 **FOURTH CAUSE OF ACTION**
12 **(RICO, 18 U.S.C. § 1962(c))**

13 182. Plaintiffs re-allege and incorporate 5AC ¶¶ 126-149, as if fully set
14 forth in this cause of action.

15 183. Defendants NDS, NDS Americas, Norris, Hasak, Kommerling,
16 Tarnovsky, Menard, Main, Dawson, Quinn, Sergei, and Frost's unlawful, tortious
17 and otherwise actionable conduct as alleged in Plaintiffs' 5AC constitutes a pattern
18 of "racketeering activity" as defined by 18 U.S.C. § 1961.

19 184. Plaintiffs' hereby incorporate by reference as if fully set forth herein
20 each separate and distinct theory of direct and indirect liability outlined above in
21 Count I of Plaintiffs' 5AC.

22 185. Defendants committed at least the following predicate acts: (i) criminal
23 copyright infringement in violation of 17 U.S.C. § 506(a) and 18 U.S.C. § 2319; (ii)
24 misconduct in connection with access devices in violation of 18 U.S.C. § 1029; and
25 (iii) mail and wire fraud in violation of 18 U.S.C. § 1341 and §1343.¹² Defendants

26 ¹² Plaintiffs acknowledge that its mail and wire fraud predicates and bases for
27 independent RICO liability were previously denied by the Court's November 5,
28 2007 Order Granting in Part and Denying in Part Plaintiffs' Motion to Reinstate
RICO Claims. Plaintiffs include these claims/allegations in its 5AC, however, for
the sole purpose of preserving appellate rights.

1 produced, trafficked in, controlled, and possessed device making equipment in
2 violation of 18 U.S.C. § 1029(a)(4).

3 186. Each of these violations by each of the foregoing Defendants of 18
4 U.S.C. §§ 1029, 1341, 1343, and 2319, constitutes an instance of “racketeering
5 activity” as defined in 18 U.S.C. § 1961(1), and was committed in furtherance of
6 the conspiracy to compromise and make available EchoStar’s proprietary
7 information to the general public for an illegal use. Each of the foregoing
8 Defendants aided and abetted the commission of these violations of 18 U.S.C. §§
9 1029, 1341, 1343, and 2319.

10 187. At all times relevant, NDS, Tarnovsky, Menard, and the distribution
11 network, (“distribution network”) were associated-in-fact through their continuing
12 efforts from as early as 1998 to present to compromise, and make available to the
13 general public for improper and illegal use, EchoStar’s proprietary information
14 including, but not limited to, EchoStar’s secret ROM and EEPROM Codes, Pirated
15 EchoStar Access Cards and other Circumvention or Signal Theft Technology and
16 Devices, and software programs, technical support services, and fixes designed and
17 intended to circumvent Plaintiffs’ ECMs that instituted primarily to disable
18 Defendants’ illegal devices and/or support services. Such association in fact
19 constitutes an enterprise as defined in 18 U.S.C. §1961(4).

20 188. Defendant NDS specifically functioned to oversee and coordinate the
21 implementation of specific acts by NDS Group, Tarnovsky, Menard, and the
22 distribution network, made strategic decisions concerning the extraction of
23 Plaintiffs’ secret ROM and EEPROM Codes, the design and manufacture of Pirated
24 EchoStar Access Cards and other Circumvention or Signal Theft Devices, and
25 facilitated communication between the various Defendants referenced herein.
26 Specifically, Defendant NDS directed the affairs of NDS Group, Tarnovsky,
27 Menard, and the distribution network on an ongoing basis and recruited and
28 attempted to recruit others for the enterprise including, but not limited to, Norm

1 Dick and John Greyson. Defendant NDS also made decisions about the
2 information that was to be made available to the general public in addition to
3 manner and timing of the release of Plaintiffs' secret ROM and EEPROM Codes,
4 select portions thereof, and/or specific and detailed instructions on how to extract
5 same, the design and manufacture of Pirated EchoStar Access Cards and other
6 Circumvention or Signal Theft Devices. This constitutes an organization separate
7 and apart from the activity in which NDS was engaged.

8 189. Defendant NDS has and had at all times relevant herein an
9 organizational structure or system of authority for making and implementing
10 decisions and for exercising common control over the members of the RICO
11 enterprise.

12 190. The organization and structure of Defendants' RICO enterprise existed
13 as an entity separate and apart from the pattern of conspiratorial racketeering
14 activity. Menard is or was at the top of the distribution and sale structure of the
15 enterprise and controls this enterprise through various business entities. These
16 business entities included, among others, DR7, a Canadian business entity
17 operating through the website www.dr7.com. DR7 has or had a legal existence
18 separate and apart from the enterprise and its illegal racketeering activity.
19 However, it is or was operated and utilized as part of the enterprise for the purpose
20 of furthering the racketeering activity. The enterprise also operates through, among
21 others, "Discount Satellite" owned and operated by Dave Dawson, "Koinvizion"
22 owned and operated by Andre Sergei, and the "NewFrontier Group" owned and
23 operated by Stanley Frost. Menard employed various associates who work directly
24 for him, assisting in the day to day operation of the DR7 website and of the
25 enterprise.

26 191. Menard is or was the primary decision-maker of the distribution and
27 sale structure of the enterprise, controlling and directing the affairs of the group on
28 an ongoing basis and recruiting the various individual Defendants and/or their

1 agents. Menard exerted control over the direction of the enterprise by, for example,
2 selling devices that allowed the pirates to operate as “dealers” of Pirated EchoStar
3 Access Cards and/or other Circumvention or Signal Theft Devices. Those
4 associated with Defendants constituted a distribution network for the Pirated
5 EchoStar Access Cards, other Circumvention or Signal Theft Devices, and
6 otherwise pirate technology. They imported, exported, concealed, and sold Pirated
7 EchoStar Access Cards to persons (DISH Network’s subscribers and prospective
8 subscribers) throughout the United States and elsewhere. They used pirate
9 technology, including reprogrammers, to manufacture Pirated EchoStar Access
10 Cards and/or other Circumvention or Signal Theft Devices and repair disabled
11 Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices
12 upon Plaintiffs’ ECMs. These actions were taken in furtherance of the enterprise’s
13 goal of harming Plaintiffs and decreasing Plaintiffs’ competitiveness in the DBS
14 and CAS marketplaces.

15 192. NDS is or was the primary decision-maker of the technology structure
16 of the enterprise, controlling and directing the affairs of Tarnovsky on an ongoing
17 basis and recruiting or attempting to recruit others for the enterprise. NDS exerted
18 control over the direction of the enterprise by, for example, employing or
19 attempting to employ individuals to hack or break the Security System, and by
20 determining what technology and information would be made available to harm
21 Plaintiffs. The enterprise is more than the sum of its racketeering activity.

22 193. The distribution side, and the technology side, of the organization and
23 structure discussed herein functioned as a continuing unit and were controlled
24 primarily by the single-decision making apparatus within NDS, which determined
25 when and what hacked software code to release to the public.

26 194. The central decision making apparatus within NDS was able to control
27 Menard and his distribution network by, *inter alia*, (a) NDS bestowing upon
28 Menard the ability to reprogram EchoStar Access Cards by providing Menard with

1 a sophisticated reprogrammer device (coined by Tarnovsky as “the stinger”)
2 designed and built by NDS and Tarnovsky using the proprietary information NDS
3 unlawfully obtained from the microprocessor embedded in Plaintiffs’ Access Cards
4 at the NDS laboratory in Haifa, Israel; (b) controlling the number of EchoStar
5 Access Cards that Menard was able to unlawfully reprogram, and ultimately
6 distribute to pirating end-users via his distribution network, by instructing and/or
7 assisting Tarnovsky in writing software codes that operated the NDS/Tarnovsky
8 reprogrammer in a controlled manner such that it would automatically become
9 disabled after reprogramming a predetermined number of EchoStar Access Cards;
10 (c) controlling Menard’s ability to ‘reactivate’ the NDS/Tarnovsky reprogrammer
11 – to wit, Tarnovsky would not send software and/or command codes to reactivate
12 the reprogramming device until instructed to do so by NDS; (d) controlling which
13 specific portions of Plaintiffs’ proprietary code that Menard could publically post
14 on his www.dr7.com website as well as when such posts could be effectuated; (e)
15 controlling the specific type, generation, or version of EchoStar Access Cards that
16 Menard was able to reprogram and ultimately provide to the pirating end-users via
17 his distribution network; (f) controlling if, when, how and where the unlawfully
18 reprogrammed EchoStar Access Cards distributed by Menard and his distribution
19 network would be reactivated and/or repaired after Plaintiffs launched an ECM to
20 disable these cards by deciding whether to provide Menard a “fix”, “update,” or
21 “counter-ECM,” among other technical support, in which to post on his website or
22 whether to have Tarnovsky physically write a new software program to repair
23 disabled Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft
24 Devices in which case Menard and his distribution network would be required to re-
25 acquire these distributed cards and load them back into the NDS/Tarnovsky
26 reprogrammer; (g) controlling the price (and conversely, the supply and demand
27 market) that Menard and his distribution network were able to distribute these
28 Pirated EchoStar Access Cards for; (h) controlling the degree of protection NDS

1 would provide and when such protection was provided to Menard and the members
2 of his distribution network by, *inter alia*, running interference with and/or
3 providing information to the Canadian RCMP; and (i) controlling when and how
4 NDS/Tarnovsky would effectuate the wide-spread compromise of Plaintiffs' CAS –
5 which ultimately occurred via Tarnovsky's December 21 and 24, 2000 posts on
6 Menard's website, among others.

7 195. Defendant NDS was also able to exercise and/or retain control over the
8 distribution structure of the RICO enterprise by using various intimidation tactics,
9 threats of civil and criminal proceedings, and monetary compensation. By way of
10 example, NDS through its officer and employee Norris directed Menard to
11 terminate his website (www.dr7.com) during a meeting between Norris and Menard
12 in early 2001. Specifically, after Norris learned that representatives from Plaintiffs
13 had met with Menard in an effort to investigate the acts outlined herein, Norris
14 immediately directed Menard to terminate his website – which was done on June
15 21, 2001. Plaintiffs are informed and believe that Norris directed Menard to
16 terminate his site and discard any and all evidence connecting same to Tarnovsky
17 and/or NDS in a continued effort by NDS to conceal its involvement in same.

18 196. Defendants knowingly produced, trafficked in, controlled, and
19 possessed “device making equipment” – any equipment, mechanism, or impression
20 designed or primarily used for making an access device or counterfeit access device
21 – in violation of 18 U.S.C. § 1029, by at least the following:

22 (a) On or about April 5, 1999, a post to the Internet by “DR7” [Menard]
23 states that Menard “visited Discount [Discount Satellite/Dawson] this aft, got
24 card reloaded with bootstrap and main.enc file and some other small one that
some program made, bat card now fully functioning.”

25 (b) On or about April 20, 1999, Dawson and Discount Satellite were
26 raided in Edmonton by the RCMP; local reports regarding Dawson's selling
27 pirated EchoStar access cards and other illegal signal theft devices on his
28 Internet website, www.dsscanada.com. Among the items confiscated were

1 illegal satellite access cards, computers, and other equipment used to program
2 access cards, approximately \$69,500 in U.S. and Canadian money orders and
3 cash, and drugs. Dawson continued to operate his illegal business in Canada
4 through another hacker website owned, operated, and maintained by him –
www.discountsatellite.com up until June 21, 2003 when it was shut down.

5 (c) On or about October 6, 1999, a post to the Internet by “Code”
6 [Tarnovsky], concerning a new circumvention or signal theft device called an
7 AVR, states “if the key servers are working correctly, you will know the new
avr key they [DISH Network] are about to switch to in advance!”

8 (d) On or about October 6, 1999, a post to the Internet by “JD” [Dawson],
9 concerning inquiry to purchase AVR devices, states “we have available to us
10 now an aftermarket avr device that will activate all channels on the Echostar
11 Dishnetwork system. It runs without the use of the original plastic card and is
12 totally supported via the internet. It is NOT an auto-update product and will
13 stop working in the event of a keychange. HOWEVER, key updates are posted
within minutes and available to all. . . . Total cost for board and programmer is
currently 150.00 usd. Or 110.00 usd for just the avr board.”

14 (e) On or about September 8, 2000, a post to the Internet by “DR7”
15 [Menard] stating “I have only honestly patched 3 times in 18 months...where do
16 they get the info they post about E3m [EchoStar hack committed by NDS by and
17 through its employees and agents – Tarnvosky, Menard, and others] being so
18 bad??...I have had one [ECM] since day one when discount [Discount
19 Satellite/Dawson] began selling and have not needed to be updated 15
times...total updates I have had are 3 and since June 1999 that has cost me
approximately 5 minutes of my time spent loading.”

20 (f) On or about November 21, 2000, a post to the Internet by
21 “Koinvizion” [Sergei] announcing that [Defendants] can now fix the “smartcard
22 not inserted correctly Error for \$50.00USD per card + the usual shipping
charges for everyone.”

23 (g) On or about December 29, 2000, a post to the Internet by “hitek” [Sean
24 Quinn], entitled “e3m cards,” states “the new group wants to sell the machines
25 now...please e-mail us and we will give you info on the machines as well as
26 where you can order it from...30 machines ready to go.”

27 197. Defendants engaged in mail fraud in violation of 18 U.S.C. § 1341
28 when Defendants transmitted, by means of United States Postal Service and/or

1 commercial interstate and foreign carriers, at least the following:

2 (a) On or about April 16, 1999, NDS letter was sent from Adams to Hasak
3 concerning, among other things, a piracy investigation of www.dr7.com and
4 "DR7" [Al Menard]. Adams states, "[s]omewhere in the loop appears
5 PINKERTON investigative Service. They at one time worked for Irdeto as well
6 as other companies. There is talk that an agency is investigating
7 DR7[Menard]."

8 (b) On or about June 18, 1999, a NDS Letter to Hasak from Adams
9 concerning NDS's hiring satellite pirates and hackers in order to "CONTROL"
10 them as well as NDS's fear of losing its contract with DirecTV to be DirecTV's
11 smart card provider.

12 (c) On or about August 2, 2000, "X-Factor, X-Factor Design [Menard's
13 company], sent a package to "CT [Tarnovsky]", through a mail account in San
14 Marcos, Texas 78666 USA. The item enclosed was described as a "Sony Play
15 Station manufactured in Japan" with tracking number "W601 911 651 5."
16 Menard sent the "expedited" with the special instructions "UPS CALL MBE 1ST
17 ON ANY SHIPPER ISSUE." The "Declaration of Contents and Shipper's
18 Letter of Instruction" states that "X-Factor, X-Factor Design" shipped the
19 package and describe the items enclosed as "one (1) Sony Psx Z, manufactured
20 in Japan, valuing \$900.00; one (1) Sony Controller, manufactured in Japan,
21 valuing \$30.00, and three (3) Sony CDs, manufactured in Japan, valuing
22 \$60.00." The remarks section of the declaration reads "Birthday Gift."
23 Tarnovsky's birthday listed on his California driver's license is xxxx xx, xxxx.

24 (d) On or about August 11, 2000, a "Declaration of Contents and
25 Shipper's Letter of Instruction" states that "Hi-Fi Exchange [Menard's
26 company]," sent one package weighing 11 pounds to "CT Electronics
27 [Tarnovsky]" through a mail account in San Marcos, TX 78666. The item
28 enclosed is described as "one (1) Technics Cassette Deck, manufactured in
Singapore valued at \$350.00."

(e) On or about August 15, 2000, a "Declaration of Contents and
Shipper's Letter of Instruction" states that "Regency Audio [Menard's
company]," sent one package weighing 10 pounds to "CT [Chris Tarnovsky]
Electronics" through a mail account in San Marcos, TX. The item enclosed is
described as "one (1) Graphic Equalizer, manufactured in the USA, valuing
\$300.00."

1 (f) On or about August 23, 2000, a "Declaration of Contents and
2 Shipper's Letter of Instruction" states that "Regency Audio [Menard's
3 company]," sent one package weighing 10 pounds to "Owner, CT [Tarnovsky]
4 Electronics," through a mail account in San Marcos, TX 78666. The item sent
5 is described as "one (1) Sony Minidisk, manufactured in the USA, valuing
6 \$350.00." The shipment was charged a \$62.78 transportation charge.

7 (g) On or about August 25, 2000, "Regency, Regency Audio [Menard's
8 company]," sent one package, with a weight of 11 pounds to "CT [Tarnovsky],"
9 through a mail account in San Marcos, Texas 78666. The item is described as a
10 "compact disc player manufactured in the USA." The tracking number on the
11 package was "W619 045 603 0." The package was sent "expedited" with the
12 special instructions "Zone 351."

13 (h) On or about August 28, 2000, "Regency, Regency Audio [Menard's
14 company]," sent one package, with an actual weight of 9 pounds to "CT
15 [Tarnovsky] Electronics," through a mail account in San Marcos, Texas 78666.
16 The item was described as a "DVD Player manufactured in the USA." The
17 tracking number on the package was "W619 045 602 1", and the package was
18 sent "expedited."

19 (i) On or about August 28, 2000, a package was sent to "Von,"
20 [Tarnovsky]" from Washburn Ct, Luling, TX 78648, with FedEx letter to
21 "Chris Tarnovsky" through a mail account in San Marcos, TX 78666. The
22 parcel was sent FedEx Priority Overnight with the tracking number "8153 1564
23 6118." The sender, "Von," has an account that will be billed to pay for the
24 shipment. The parcel was to be delivered by August 29, 2000.

25 (j) On or about August 29, 2000 a package was sent to "Von"
26 [Tarnovsky] " from Mail & More in San Marcos, Texas 78666 with a FedEx
27 Envelope/Letter to "Chris Tarnovsky,XXX XXXX XXX, XXX XXXX, CA
28 XXXXX." The parcel was sent FedEx Priority Overnight with the tracking
number "8213 3536 0680." Tarnovsky, "Von," has an account, number 1700-
1825-7 that is billed for the shipment. The FedEx tag is marked "XENIRA."

(k) On or about August 29, 2000, an investigation by a Detective at the
Hays County Narcotics Task Force was conducted in response to an anonymous
call from a concerned citizen stating that a suspicious parcel had been mailed
from Luling, Texas to XXX XXXX, Texas, and then forwarded to XXX XXXX,
California at Tarnovsky's expense. The caller advised "there was no reason for
the parcel to be mailed to San Marcos, TX before being mailed to XXX XXXX,
CA." The investigation revealed that the return address and phone number on

1 this parcel was invalid. The name for the return address was "Von"
2 [Tarnovsky]. The investigation further revealed that Chris Tarnovsky was living
3 at XXX XXX XXXX, XXX XXXX, California XXXXX. On July 29, 2000, he
4 rented mailbox number 245 at "Mail and More, 925 E.HWY 80, San Marcos,
5 Hays County, Texas." In doing so, Tarnovsky falsely told the store manager
6 that he was a student at Southwest Texas State University and was returning
7 home to XXX XXXX, CA. However, there was no record of Tarnovsky ever
8 attending Southwest Texas State University or living in the San Marcos, TX
9 area. Tarnovsky instructed the store manager to forward all of his mail as
10 arriving next day including Saturday to XXX XXX XXXX, XXX XXXX,
11 California XXXXX. The store manager had been forwarding parcels to
12 Tarnovsky approximately "every day or every other day."

13 (l) On or about August 30, 2000, the store manager notified the
14 investigating detective that he received another parcel to be forwarded to
15 Tarnovsky. The parcel was in a JVC compact disc box with a return address of
16 "Regency Audio [Menard's company]," and addressed to "CT [Tarnovsky]
17 Electronics," in San Marcos, Texas. Canines gave a positive alert at the
18 presence of the odor of marijuana or other illegal drugs after smelling the
19 parcel. A search warrant was then executed and \$20,100.00 in US currency was
20 discovered inside a medium brown envelope taped to the circuitry inside the
21 JVC compact disc player.

22 (m) On or about August 31, 2000, the store manager again notified the
23 investigating detective that a parcel had arrived. The parcel was identical to the
24 one received the day before, except the box was from a "Pioneer DVD."
25 Canines again gave a positive alert at the suspected parcel. A second search
26 warrant was executed and \$20,000.00 in US currency was found in a medium
27 sized envelope taped to the circuitry of the DVD player.

28 (n) On or about December 1, 2000, a post to the Internet by "Kingtut"
stating "I just got my cards from koin [Andre Sergei]."

(o) On or about January 9, 2002, Norris purchased a "Karl Suss Probe"
manufactured by K&S, model 4524, serial number 610009, with a manual, for
the amount of \$18,500 for Tarnovsky. On or about January 17, 2002, the item
was shipped via Atlas Van Lines to "Chris Tarnovsky at XXXX XXXX XXXX,
XXXXX, California USA XXXXX, phone number xxx-xxx-xxxx, fax number
xxx-xxx-xxxx." The invoice lists the "End User" to be Chris Tarnovsky at the
same address.

1 (p) On or about July 26, 2002, Tarnovsky purchased a manufactured "Karl
2 Suss, model PM-8" for the amount of \$15,000. On or about August 15, 2002,
3 the item was shipped via Federal Express to Chris Tarnovsky at XXXX XXXX
4 XXXX, XXXXX, California USA XXXXX, phone number xxx-xxx-xxxx, fax
number xxx-xxx-xxxx. The invoice lists the "End User" to be Chris Tarnovsky.

5 (q) On or about August 30, 2002, Norris purchased a "Karl Suss Probe (2
6 units), \$1,700" and had them sent to Tarnovsky. One item, manufactured by
7 Karl Suss, was a model Probe for the amount of \$850. The other item was also
8 manufactured by Karl Suss and is a model Probe for the amount of \$850. On
9 August 30, 2002, the items were shipped via Federal Express to "Chris
10 Tarnovsky at XXXX XXXX XXXX, XXXXX, California USA XXXXX, phone
number xxx-xxx-xxxx, fax number xxx-xxx-xxxx." The invoice lists the "End
User" to be Chris Tarnovsky.

11 198. Defendants engaged in wire fraud in violation of 18 U.S.C. § 1343
12 when Defendants repeatedly used interstate and international wire facilities,
13 including telephone and Internet communications, by at least the following:

14 (a) On or about November 20, 1998, a post to the Internet by "DR7"
15 [Menard], concerning the EchoStar hack, states: "a file was sent too me recently
16 by Swiss cheese boys [Tarnovsky] and they asked me too add, lins too it are in
17 todays news 11.20.98 and it is also added to the Echostar tools section, sorry I
18 didn't have more info with this text file but I think a few of you could use this
19 info...thanks again too the Users of this forum who have contributed their time
to the Echostar Project as well as the SCP [Tarnovsky] for initiating this...good
luck guys and hope to have more info shortly."

20 (b) On or about December 4, 1998, a post to the Internet by "Nipper"
21 [Tarnovsky] providing Plaintiffs' Bat keys.

22 (c) On or about December 7-8, 1998, a post to the Internet by "Nipper"
23 [Tarnovsky] supplying illegally obtained information concerning DISH
24 Network.

25 (d) On or about March 26, 1999, a post to the Internet by "DR7" [Menard]
26 states: "the CAM dump is posted in the Tools section... Echostar Running Card
Dump + Public Keys by Swiss Cheese Productions [Tarnovsky]"

27 (e) In or around April 1999, Menard telephoned Scullion again to solicit
28 Scullion's participation in a distribution network to sell Pirated EchoStar Access

1 Cards. During this conversation, Menard informed Scullion that he was close to
2 receiving a full hack of the EchoStar system and that, "due to the pirate
3 community's interest in Swiss Cheese Production's stuff," the plan was a
4 guaranteed money maker. Menard also informed Scullion that the distribution
5 network was going to have something special attached with its operation:
6 protection of NDS. Menard informed Scullion that "NDS was the entity whom
7 had ordered the hack and the distribution of pirated cards through Menard's
8 distribution network." Menard also informed Scullion that "NDS had an
9 arrangement with Tarnovsky to provide the support and facilitation of the
10 hacked EchoStar code to be sent to Menard to be used in the distribution
11 network." Menard also informed Scullion that Scullion had nothing to worry
12 about with respect to being raided by the RCMP due to the fact that "NDS was
13 connected and had a solid relationship [with the RCMP]." Menard further
14 informed Scullion that "NDS would be running interference in the distribution
15 network."

16 (f) On or about April 10, 1999, a post to the Internet by "DR7" [Menard]
17 where he inserts a private chat he had with "CanBert" including "went to jd's
18 [Dawson] today; if I send my batt [illegal battery card] in how much to get it
19 fixed?"; not sure...never heard the price when I was there...customers pay \$40;
20 you'll have to call; at Discount Sat?"; yes 780-448-1787; thankx DR7; np man."

21 (g) May 9, 1999, a post to the Internet states that the "Echostar update for
22 the commercial battery cards has been released and is confirmed working again.
23 The file can be downloaded from [Dawson's website]
24 www.discountsatellite.com/Efile.zip."

25 (h) On or about May 19, 1999, a post to the Internet by "DR7" [Menard]
26 states that he asked JD [Dawson] why the bat [battery card] isn't autorolling
27 [automatically finding keys to counter ECMS]. JD [Dawson] stated the reason
28 was the requirement to hand out a bootstrap and that the potential source code
would have to be released.

(i) In April 1999, Menard telephoned Reginald Scullion with an offer to
participate in the "DISH Network" hack. During these conversations, Menard
informed Scullion that, among other things: (a) NDS was behind the EchoStar
hack; (b) the Tarnovsky/Menard distribution model would be protected and
controlled by NDS; (c) NDS had an arrangement with Tarnovsky to provide the
technical and software support and facilitate the hacked EchoStar ROM Code to
be sent to Menard and used in the distribution network; and (d) NDS would
protect this distribution network from potential RCMP raids.

1 (j) On or about July 6, 1999, a post to the Internet by "DR7" [Menard]
2 states that "marry3M is used for JD's [Dawson's] 3M customers to do the
3 following: Write IRD# Write Key# Read Key# from card with sub/previous sub
Set zipcode/timezone."

4 (k) On or about August 10, 1999, a post to the Internet by "Nipper"
5 [Tarnovsky] providing EchoStar Bat keys.

6 (l) On or about August 21, 1999, a post to the Internet by "DR7"
7 [Menard] states that Menard called "JD" [Dawson] to confirm status of file and
8 JD [Dawson] stated that he would "post REV20A.E3M on his website."

9 (m) On or about September 8, 1999, a post to the Internet by "xbr21"
10 [Tarnovsky], quoting "Nipper's" [Tarnovsky's] previous post, stating "here is a
11 neat no-mod trick- send out a control work packet using a key offset of 07 (eg
12 05/15/07). Card should skip decript of packet and simply encrypt with your
boxkey!! Simple and why not use this on channel 101? Another example of
stupidity."

13 (n) On or about September 29, 1999, a post to the Internet by "DR7"
14 [Menard] states that he talked to "JD" [Dawson] on the phone about 20 minutes
15 ago and JD [Dawson] said that he would also just "sell the programmed [DISH
16 Network] chip" if there was a demand for it. A later post to the Internet, on the
17 same date, by "DR7" [Menard] stating that he "confirmed with JD [Dawson]
that the keys in the latest talk.cfg file are not for AVR freeware and will only
work on JD's [Dawson's] AVR."

18 (o) On or about October 19, 1999, a post to the Internet by "DR7"
19 [Menard] announced that "'xfile 2.01' and 'Blocker version 2.3 Beta' were
20 posted to the Echo files section of the DR7 website." "DR7" [Menard] further
21 states "sorry they were not posted earlier but the creators
22 [Defendants/Tarnovsky] never bothered to send them so basically I couldn't post
what I didn't have, thanks to those that did send them."

23 (p) In November 1999, Menard again telephoned Reginald Scullion with
24 an offer to participate in the "DISH Network" hack. During these conversations,
25 Menard informed Scullion that, among other things: (a) NDS was behind the
26 EchoStar hack; (b) the Tarnovsky/Menard distribution model would be
27 protected and controlled by NDS; (c) NDS had an arrangement with Tarnovsky
28 to provide the technical and software support and facilitate the hacked EchoStar
ROM Code to be sent to Menard and used in the distribution network; and (d)
NDS would protect this distribution network from potential RCMP raids.

1
2 (q) On or about November 9, 1999, a post to the Internet by "DR7"
3 [Menard], regarding "JD's [Dawson's] gone???", states "since Friday I have not
4 been able at all to call your shop and get through, I tried over 20 times per day at
5 least just to test. JD [Dawson] this is getting outta hand and now its come to the
6 point where I am looking bad for advertising for you and also for being in same
7 city, I think you owe these people an explanation as well as an apology and
8 shouldn't expect me to have to deal with any of this...I an now removing
Discount Satellite advertising banners from this website JD [Dawson] because I
cannot and will not give you [Dawson] any more benefits that other advertisers
and make myself look bad in the process.

9 (r) On or about November 19, 1999, a post to the Internet by "DR7"
10 [Menard] provides instructions to remedy problem of member who received an
11 AVR2 [smart card replacement] and programmer [device used to program
12 Access Cards or illegal substitute cards] and was unable to load properly.
"DR7's" [Menard's] instructions include, "using DOS talk v1.7 and loading the
avr2e3m [EchoStar] file which allows AVR2 to use the 3M keys from wintalk."

13 (s) On or about December 8, 1999, a post to the Internet by "Shrimp"
14 [Tarnovsky] states "the sole purpose of the Atmel chip in the wildthing is a slave
15 who can count clock cycles and perform a high glitch on vcc/clk given a
16 command from the PC. All that is required to fix the current situation is a new
.exe file given different glitches to the card."

17 (t) On or about December 17, 1999, a post to the Internet by "Nipper-
18 Clauz" [Tarnovsky], entitled "Twas the Night Before Christmas," provided
EchoStar Bat keys.

19 (u) On or about December 20, 1999, a post to the Internet by "Nipper-
20 Clauz" [Tarnovsky] entitled "tis the season to be jolly," provided additional
21 EchoStar Bat keys.

22 (v) On or about December 21, 1999, a post to the Internet by "Nipper-
23 Clauz" [Tarnovsky] entitled "be merry harry," provided even more EchoStar Bat
24 keys.

25 (w) On or about February 2, 2000, Dawson and Discount Satellite were
26 raided a second time by the RCMP after local reports regarding
27 Dawson's continued selling of pirated DSS and EchoStar access cards and other
28 illegal signal theft devices on the Internet through his website,
www.discountsatellite.com.

1 (x) On or about February 25, 2000, a post by "NiPpEr" [Tarnovsky] to the
2 internet providing EchoStar Bat keys.

3 (z) On or about March 29, 2000, DirecTV executed and seized Dawson's
4 business in satisfaction of the judgment obtained by DirecTV against Dawson.
5 Shortly thereafter, Dawson posted a public statement on his website,
6 www.discountsatellite.com, regarding the status of his business's operations.
7 Included in this statement, Dawson provided a link to www.DSScanada.com,
8 another website owned, operated, and maintained by Dawson. Through this
9 website, Dawson continued to solicit business from his large customer base in
10 addition to new customers.

11 (aa) On or about May 5, 2000, an NDS Memorandum captioned "Report
12 Week 18", concerning NDS agent Christopher Tarnvosky, states in relevant
13 part: "You will note that suspicion has fallen on MIKE [Tarnovsky]... There are
14 a series of threatening statements inasmuch that MIKE [Tarnovsky] is behind
15 DR7 [Allen Menard and the website www.dr7.com] and therefore MIKE
16 [Tarnovsky] hacked ECHOSTAR etc, etc."

17 (ab) On or about June 21, 2000, a post to the Internet by "Hitec" [Quinn],
18 concerning "Koin" [Sergei], states "[f]or the time being... I am removing all
19 dealer links from the site... Koin is closing the website but still accepting orders
20 at Koin@koinvision.com . . . now its cash (no money orders at all) and no
21 site.... Any other files that are required to help out the Koinster will be posted
22 here from now on."

23 (ac) On or about June 27, 2000, a post to the Internet by "Hitec" [Quinn],
24 concerning business operations of Koin [Sergei], stating "Koin [Sergei] is
25 closing the website but still accepting orders at Koin@Koinvision.com . . . My
26 self I personally vouch for Koin and his support. Even with his one complaint
27 the guy has to admit that Koin did send his package originally (although it was
28 seized) and he did make up for it after a couple of weeks . . . Any other files that
29 are required to help out the Koinster will be posted here [www.hitecsat.com]
30 from now on." A later post on the same date by "Hitec" [Quinn] stating "as I
31 already said . . . no money order now and only email . . . I will post any files
32 needed to help out Koin [Sergei]. His email addy again is
33 Koin@koinvizion.com."

34 (ad) On or about August 15, 2000, a post by "HeeD" states "the group that
35 is supporting DN E3M [the illegal DISH Network hack] has proven that they
36 know this system inside-and-out. They are not just taking stabs in the dark, or
37 speculating about things...they actually know!"

1
2 (ae) On or about September 19, 2000, it was discovered that Tarnovsky
3 placed approximately 80 phone calls to Israel [NDS] and 120 to Belgium.
4 Tarnovsky also traveled overseas twice every six months going to Brussels and
5 other European countries. Tarnovsky had received two parcels at his residence
6 from Minnesota and Virginia [Tarnovsky Sr.].

7 (af) On or about November 21, 2000, a post to the Internet by
8 "Koinvizion" [Sergei] announcing that [Defendants] can now fix the "smartcard
9 not inserted correctly Error for \$50.00USD per card + the usual shipping
10 charges for everyone."

11 (ag) On or about December 21, 2000, Tarnovsky, using the alias "nIpPeR
12 cLaUz 00", published a file entitled "nipperclauz.txt" on Menard's website
13 which consisted of a hack methodology for defeating EchoStar's security
14 system. In his post Tarnovsky states: "there will be no boxes anymore! There
15 will be no more fights amongst us. Learn from this and prosper. Works across
16 the world! Do the following: get atr, wait 500ms to ensure card is idle. Send this
17 packet to 288-02 or equivalent ROM 3 nagra cam! Rx 4+4096 bytes and you
18 have entire eeprom. Send this, then rx 4 bytes + 4096 bytes of eeprom." The
19 post was signed by "nIpPeR cLaUz 00" [Tarnovsky]. This December 21, 2000
20 post by Tarnovsky provided hackers around the world the 'road map' and
21 instructional code to effectuate a complete dump of Plaintiffs' entire EEPROM
22 Code and exploit vulnerabilities in Plaintiffs' CAS which could be leveraged to
23 attack and hack EchoStar's security system.

24 (ah) On December 24, 2000, a post to the Internet by "NiPpEr2000"
25 [Tarnovsky] at 3:26 a.m. publishing the FULL Echo ROM Code on
26 www.piratesden.com, Discussion Forum. "NiPpEr2000" [Tarnovsky's] post,
27 entitled "tHe ReAl V3 DuMp!," stating "tHeRe WiLl bE nO bOxES aNyMoRe!
28 tHeRe WiLl bE nO mOrE fIghTInG aMoNgSt uS. LeArN fRoM ThIs aNd
pRosPer. tHiS WiLl Be PoStEd To ALL NeWsGrOuPs ArOunD ThE WoRiD!
ThIs Is Dr7'S cOdE (WeSt 3M v3) tHe rEaL sTuFf!!" Tarnovsky then goes on
to state: "I wILL dUmP ALL vErSiOnS oF tHe WeSt CoDe LoOk FoR iT hErE!
nIpPeR cLaUz 00" [Tarnovsky].

(ai) On or about May 18, 2001, a post to the Internet by "Kelly" [Menard]
stating "we all do know "Hitec" [Quinn] and "Koin" [Sergei] were partners
selling echostar stuff...I bought my avr and echostar 3m from you [Quinn] and
that bitch koin [Sergei].

1 (aj) On or about May 18, 2001, a post to the Internet by "Hitec" [Quinn],
2 responding to "Kelly's" [Menard's] allegations, stating "if I was involved in the
3 Echostar hack I would have forced the price down to an affordable rate instead
4 of lying to dealers and constantly gouging them. If memory serves me correctly
5 I even advertised for the competition that did force the price down
6 considerably."

6 (ak) On or about December 16, 2001, Tarnovsky admits to Giles Kaehlin,
7 Head of Security for Canal+, at a meeting in London that NDS was responsible
8 for the hack and publication of the DISH Network ROM Code on the internet.
9 Tarnovsky admits that the DISH Network code was sent to him by Reuven
10 Hasak, head of security for NDS in Israel, from John Norris, head of security for
11 NDS Americas. Tarnovsky later sent an email stating that he wanted no further
12 communications to occur between himself and Kaehlin.

11 199. Defendants willfully infringed on EchoStar's copyrighted
12 information for purposes of commercial advantage, in violation of 17 U.S.C. § 506
13 and 18 U.S.C. § 2319.

14 200. Alternatively, Defendants specifically used their positions at
15 NDS to conduct or participate, directly or indirectly, in the conduct of NDS's
16 affairs, in violation of 18 U.S.C. §§ 1029, 1341, 1343, and 2319 by, among other
17 unlawful acts, engaging in the conduct specifically set forth above.

18 201. The multiple acts of racketeering activity as set forth above by
19 Defendants and their employees, agents, sub-agents and/or co-conspirators were
20 interrelated, part of a common and continuous pattern of fraudulent schemes, and
21 perpetrated for the same or similar purposes, thus constituting a "pattern of
22 racketeering activity," as defined in 18 U.S.C. § 1961(5).

23 202. By reason of these circumstances and events, Defendants
24 agreed to and/or did conduct and participate, directly and indirectly, in the conduct
25 of the affairs of the enterprise through a pattern of racketeering activity, in violation
26 of 18 U.S.C. § 1962(c).

27 203. Defendants' violations have injured and will continue to injure
28 EchoStar by depriving them of subscription and pay-per-view revenues and other

1 valuable consideration, compromising EchoStar's security and accounting systems,
2 infringing on EchoStar's trade secrets and proprietary information, interfering with
3 EchoStar's contractual and prospective business relations, and damaging Plaintiffs'
4 reputation in the DBS and CAS marketplaces resulting in, among other injuries,
5 irreparable harm to the commercial goodwill that Plaintiffs have established in the
6 relevant industries.

7 **FIFTH CAUSE OF ACTION**
8 **(Unfair Competition, Cal. Bus. & Prof. Code § 17200)**

9 204. Plaintiffs re-allege and incorporate FAC ¶¶ 152-180 above, as if
10 fully set forth in this cause of action.

11 Defendant NDS Americas

12 205. Defendant NDS Americas engaged in unlawful or unfair
13 business acts or practices by engaging in the conduct stated in (5AC ¶¶ 12-27, 38-
14 48, 82-85, 89-97, 101-106, 118, 119, 182-203 & incorporated citations).

15 Defendant NDS Group

16 206. Defendant NDS Group engaged in unlawful or unfair business
17 acts or practices by engaging in the conduct stated in (5AC ¶¶ 12-27, 38-48, 82-85,
18 89-97, 101-106, 118, 119, 183-204 & incorporated citations).

19 207. Defendants' violations of this statutory provision caused injury
20 to Plaintiffs in the district, the State of California, the United States, and elsewhere.

21 208. NDS Americas and its employees/agents Tarnovsky and Menard
22 willfully, unlawfully, and according to a plan, with the intention of harming
23 Plaintiffs, acquired EchoStar Access Cards.

24 209. Defendants' invasive attack of EchoStar's Access Cards,
25 dissemination of the information about the Security System and assistance to
26 Menard and his network of distributors was intentional and done for the wrongful
27 purpose of inhibiting competition in the industry and unfairly benefiting
28 Defendants. As a direct and proximate result of Defendants' violations of Section

1 17200, Defendants have been unjustly enriched at Plaintiffs' expense. Defendants'
2 and/or their agents have taken money from Plaintiffs in the form of lost business
3 opportunity from subscription sales to persons that, instead, used pirated Access
4 Cards to receive DISH Network programming without paying the subscription
5 price. Plaintiffs therefore have an ownership in the unjust profits received by
6 Defendants and/or their agents. Plaintiffs are entitled to recover restitution of any
7 and all of Plaintiffs' property including, but not limited to, EchoStar Access Cards,
8 Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft
9 Devices, unlawfully obtained or possessed by Defendants and/or their agents.
10 Plaintiffs are also entitled to restitution on behalf of their customers who were
11 misled and defrauded by Defendants' actions. Plaintiffs are also allowed to
12 recover monetary damages to be paid from Defendant to Plaintiff to the extent that
13 Defendants have directly taken money or property from Plaintiffs.

14 210. Defendants violated this statutory provisions within the State
15 of California.

16 211. As a direct and proximate result of each of the foregoing
17 Defendants' violations of Section 17200, Plaintiffs have suffered and will continue
18 to suffer irreparable harm, including but not limited to harm to their business
19 reputations, and goodwill. Therefore, Plaintiffs' remedy at law is inadequate and
20 Plaintiffs are entitled to an injunction prohibiting Defendants from taking any steps
21 to contribute to the copying of any of Plaintiffs' software code or any steps to
22 reverse engineer, hack, or otherwise violate any technological measure on any
23 EchoStar Access Card or any other aspect of Plaintiffs' CAS, as well as other
24 remedies to which Plaintiffs may prove themselves entitled at trial.

25
26
27 **SIXTH CAUSE OF ACTION**
28 **(Violation of California Penal Code § 593d(a))**

1 212. Plaintiffs re-allege and incorporate 5AC ¶¶ 126-149, as if fully set
2 forth in this cause of action.

3 213. Defendants violated California Penal Code § 593d(a) by knowingly
4 and willfully: (1) making or maintaining unauthorized connections to EchoStar's
5 DBS system or Plaintiffs' Security System, or any components thereof; (2)
6 purchasing, possessing, attaching, causing to be attached, assisting others in
7 attaching, or maintaining the attachment of unlawfully reprogrammed EchoStar
8 Access Cards or other Signal Theft Devices to EchoStar's DBS system or
9 Plaintiffs' Security System; (3) making or maintaining any modification or
10 alteration to EchoStar Access Cards without authorization from EchoStar; or (4)
11 obtaining and using unlawfully reprogrammed EchoStar Access Cards or other
12 Signal Theft Device to obtain EchoStar Programming without authorization:

13 Defendant NDS Group

14 214. Defendant NDS Group are secondarily liable for the unlawful acts of
15 Defendant NDS Americas and its employees (Norris and Tarnovsky), Menard, the
16 "dealers" in the NDS/Tarnovsky/Menard distribution network and other persons
17 committed in violation of Cal. Penal Code 593d(a)(1)-(4) by engaging in the
18 conduct stated in (5AC ¶¶ 12-27, 38-48, 82-85, 89-97, 101-106 & incorporated
19 citations) under the theories advanced therein.

20 Defendant NDS Americas

21 215. Defendant NDS Americas violated Cal. Penal Code 593d(a) by and
22 through its employees Norris and Tarnovsky engaging in the conduct stated in
23 (5AC ¶¶ 16-18, 39-48, 84-97, 118, 119 & incorporated citations).

24 216. Defendant NDS Americas is also secondarily liable for the unlawful
25 acts of Menard, the "dealers" in the NDS/Tarnovsky/Menard distribution network
26 and other persons committed in violation of Cal. Penal Code 593d(a) by engaging
27 in the conduct stated in (5AC at ¶¶ 12-27, 38, 84-97, 101-106 & incorporated
28 citations) under the theories advanced therein.

1 217. EchoStar is a “multichannel video or information provider” within the
2 meaning of California Penal Code § 593d(i).

3 218. Defendants’ acts constituting violations of California Penal Code §§
4 593d(a)(1)-(4) have been and continue to be performed without the permission,
5 authorization, or consent of Plaintiffs.

6 219. Defendants’ violations have injured, and will continue to injure,
7 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
8 other valuable consideration, compromising Plaintiffs’ security and accounting
9 systems, infringing Plaintiffs’ trade secrets and proprietary information, and
10 interfering with Plaintiffs’ contractual and prospective business relations.

11 220. Defendants’ violations of California Penal Code §§ 593d(a)(1)-(4)
12 were done knowingly and willfully, and for the purpose of commercial advantage
13 or private financial gain. EchoStar is entitled to recover, under California Penal
14 Code § 593d(f), the greater of three times its actual damages, or statutory damages
15 of \$5,000 for each violation of California Penal Code §§ 593d(a)(1)-(4). Plaintiffs
16 are also entitled to recover reasonable attorneys’ fees. California Penal Code §
17 593d(f)(2).

18
19 **SEVENTH CAUSE OF ACTION**
(Violation of California Penal Code § 593e(b))

20 221. Plaintiffs re-allege and incorporate 5AC ¶¶ 126-149 as if fully
21 set forth in this cause of action.

22 222. Defendants violated California Penal Code § 593e(b) by
23 knowingly and willfully providing a device, plan, or kit for a device (including but
24 not limited to unlawfully reprogrammed EchoStar Access Cards and a methodology
25 for hacking EchoStar’s Security System) designed in whole or in part to descramble
26 or intercept or otherwise make intelligible EchoStar’s satellite television
27 programming transmission signal without the express authorization of EchoStar:
28

1 Defendant NDS Group

2 223. Defendant NDS Group is secondarily liable for the unlawful acts
3 committed by Defendants NDS Americas and its employees Norris, Tarnovsky,
4 Menard and the “dealers” in the NDS/Tarnovsky/Menard distribution network and
5 other persons in violation of California Penal Code § 593e(b) by engaging in the
6 conduct stated in (5AC ¶¶ 12-27, 38-48, 82-85. 89-97, 101-106 & incorporated
7 citations) under the theories advanced therein.

8 Defendant NDS Americas

9 224. Defendant NDS Americas violated California Penal Code §
10 593e(b) by engaging in the conduct stated in (5AC ¶¶ 16-18, 39-48, 84-97, 118, 119
11 & incorporated citations).

12 225. Defendant NDS Americas is secondarily liable for the unlawful
13 acts and/or omissions of Menard, the “dealers” in the NDS/Tarnovsky/Menard
14 distribution network and other persons committed in violation of California Penal
15 Code §593e(b) by engaging in the conduct stated in (5AC at ¶¶ 12-27, 38, 84-97,
16 101-106 & incorporated citations) under the theories advanced therein.

17 226. EchoStar is a “subscription television system” within the
18 meaning of California Penal Code § 593h(1).

19 227. EchoStar’s satellite transmission of television programming is
20 an “encoded, scrambled, or other nonstandard signal” within the meaning of
21 California Penal Code § 593e(g).

22 228. Defendants’ acts constituting violations of California Penal
23 Code § 593e(b) have been, and continue to be, performed without the permission,
24 authorization, or consent of Plaintiffs.

25 229. Defendants’ violations have injured, and will continue to injure,
26 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
27 other valuable consideration, compromising Plaintiffs’ security and accounting
28 systems, infringing Plaintiffs’ trade secrets and proprietary information, and

1 interfering with Plaintiffs' contractual and prospective business relations.

2 230. Defendants' violations of California Penal Code § 593e(b) were
3 committed knowingly and willfully, and for the purpose of commercial advantage
4 or private financial gain.

5 231. Due to Defendants' wrongful conduct, Plaintiffs are entitled to
6 either: (i) statutory damages in an aggregate amount of not less than \$500 or more
7 than \$10,000 for each unlawful device; or (ii) three times the amount of actual
8 damages sustained by Plaintiffs as a result of Defendants' violations of California
9 Penal Code § 593e(b) in addition to any revenues which have been obtained by
10 Defendants as a result of Defendants' violations thereof, or (iii) an amount equal to
11 three times the value of the services unlawfully obtained by Defendants, or the sum
12 of \$500 for each unauthorized signal theft device manufactured, sold, used, or
13 distributed. Cal. Penal Code § 593e(c)(2)).

14 232. Because Defendants' violations of California Penal Code §
15 593e(c) were committed knowingly and willfully and for purposes of commercial
16 advantage or private financial gain, the Court may increase the award of damages,
17 whether actual or statutory, by an amount of not more than \$50,000. Because of
18 Defendants' violations of California Penal Code § 593e(c) were committed
19 knowingly, willfully, and wantonly, punitive damages are appropriate under
20 California Penal Code § 593e(c)(2). Plaintiffs are also entitled, under California
21 Penal Code § 593e(d), to its full costs plus an award of reasonable attorney's fees.

22
23 **PRAYER FOR RELIEF**

24 **WHEREFORE**, Plaintiffs seek a judgment against Defendants as follows:

25 A. Find that Defendants' conduct in designing, developing, manufacturing,
26 assembling, modifying, importing (to the United States), exporting, distributing,
27 selling, advertising for sale, trafficking in, and providing software, information, and
28 technical support services related to Pirated EchoStar Access Cards and other

1 Circumvention or Signal Theft Technology and Devices intended to facilitate the
2 illegal and unauthorized reception and use of EchoStar's satellite television
3 programming services by persons not authorized to receive such programming
4 violates 47 U.S.C. §§ 605(a), 17 U.S.C. §1201(a)(1)(A) and § 1201(a)(2), 18
5 U.S.C. §§ 1962(c), California Business and Professions Code § 17200, California
6 Penal Code § 593d(a)(2) and § 593e(b);

7 B. Find further that Defendants' violations were willful, for a tortious or illegal
8 purpose, or for purposes of direct or indirect commercial advantage or private
9 financial gain;

10 C. In accordance with 47 U.S.C. § 605(a), 17 U.S.C. § 1203(b)(1), 18 U.S.C. §
11 1964(a), California Business and Professions Code § 17206, and California state
12 law, enjoin and restrain Defendants and persons or entities controlled directly or
13 indirectly by Defendants from: (a) designing, manufacturing, assembling,
14 modifying, importing (to the United States), trafficking, possessing, distributing, or
15 selling Pirated EchoStar Access Cards and other Circumvention or Signal Theft
16 Devices; (b) assisting, procuring, or aiding and abetting any persons in the
17 unauthorized reception and use of EchoStar's satellite television Programming; (c)
18 advertising for sale Pirated EchoStar Access Cards and other Circumvention or
19 Signal Theft Technology and Devices; or (d) providing software, information, or
20 technical support services relating to (1) Pirated EchoStar Access Cards, (2) other
21 Circumvention or Signal Theft Devices, or (3) the illegal and unauthorized
22 reception and use of EchoStar's satellite television Programming by persons not
23 authorized to receive such programming;

24 D. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), and California Business &
25 Professions Code § 17206, grant an Order directing Defendants to return to
26 Plaintiffs all trade secrets, proprietary information, Pirated EchoStar Access Cards,
27 other Circumvention or Signal Theft Devices, and any other hardware or software
28

1 derived from EchoStar Access Cards, Plaintiffs' Security System, and EchoStar's
2 satellite television Programming service;

3 E. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), 18 U.S.C. § 2520(b)(1), and
4 California Business & Professions Code § 17206, grant an Order impounding all
5 Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in
6 the possession, custody, or control of Defendants, or related entities of Defendants,
7 that the Court has reasonable cause to believe were involved in a violation of any
8 causes of action alleged herein;

9 F. Grant an Order requiring Defendants to post a prominent public notice on
10 any Internet website owned, operated, or maintained by Defendants notifying all
11 persons in possession of Pirated EchoStar Access Cards or other Circumvention or
12 Signal Theft Devices that said Access Cards and devices have been recalled and
13 must be returned to Plaintiffs;

14 G. Grant an Order requiring Defendants to identify all John Does working in
15 concert with Defendants in performing the unlawful acts described herein, and to
16 use all contact information in Defendants' possession, custody, or control to notify
17 anyone who has obtained a Pirated EchoStar Access Cards or other Circumvention
18 or Signal Theft Devices from Defendants that said Access Cards and devices have
19 been recalled and must be returned to Plaintiffs;

20 H. Grant an Order directing Defendants to preserve and maintain all records, in
21 any form (including electronic form), that evidences, refers to, or relates to: (a)
22 EchoStar Access Cards; (b) Plaintiffs' encryption technology; (c) Pirated EchoStar
23 Access Cards; (d) other Circumvention or Signal Theft Technology and Devices;
24 (e) communications or correspondence with manufacturers, suppliers, distributors,
25 or customers of Pirated EchoStar Access Cards or other Circumvention or Signal
26 Theft Devices, or access card programming services; (f) the identity of any
27 manufacturers, suppliers, distributors, or customers of Pirated EchoStar Access
28 Cards or other Circumvention or Signal Theft Devices; and (g) the quantity of

1 Pirated EchoStar Access Cards, including EchoStar Access Cards that have not yet
2 been altered, pirated, modified, compromised, and/or counterfeited, and other
3 Circumvention or Signal Theft Devices in inventory and sold by Defendants;

4 I. Grant an Order permitting Plaintiffs, through its counsel, to inspect and make
5 mirror image copies of any computer or electronic storage drives or back-up tapes
6 in the possession, custody, or control of Defendants or related entities that contain
7 information that evidences, refers to, or relates to Defendants' conduct of
8 designing, developing, manufacturing, assembling, modifying, importing (to the
9 United States), exporting, trafficking, distributing, and selling Pirated EchoStar
10 Access Cards or other Circumvention or Signal Theft Technology and Devices, or
11 providing software, information, or technical support services relating to Pirated
12 EchoStar Access Cards or other Circumvention or Signal Theft Technology and
13 Devices designed to facilitate the illegal and unauthorized reception and use of
14 EchoStar's satellite television Programming services by persons not authorized to
15 receive such programming;

16 J. Grant an Order requiring Defendants to file with the Court and to serve on
17 counsel for Plaintiffs, within 30 days from entry of the injunction, a report in
18 writing under oath setting forth in specific detail the manner and form in which
19 each respective Defendant has complied with the injunctions and orders described
20 in paragraphs A through I above;

21 K. In accordance with 47 U.S.C. §§ 605(e)(3)(C)(i) and (ii), award Plaintiffs the
22 greater of (a) its actual damages together with any profits made by Defendants that
23 are attributable to the violation alleged herein, or (b) statutory damages in the
24 amount of up to \$110,000 for each violation of 47 U.S.C. § 605(a);

25 L. In accordance with 18 U.S.C. § 1964(c), award Plaintiffs treble the amount of
26 actual damages suffered by Plaintiffs in their business or property by reason of
27 Defendants' violations of 18 U.S.C. §§ 1964(c);

28

1 M. In accordance with California Penal Code § 593d, award Plaintiffs the greater
2 of (a) three times the amount of actual damages suffered by Plaintiffs in their
3 business or property by reason of Defendants' violations of California Penal Code §
4 593d(2), or (b) statutory damages in the amount of up to \$5,000 for each violation
5 of California Penal Code § 593d.

6 N. In accordance with California Penal Code § 593e, award Plaintiffs the greater
7 of: (a) three times the amount of actual damages suffered by Plaintiffs in their
8 business of property by reason of Defendants' violations of California Penal Code §
9 593e(b), or (b) statutory damages in the amount of up to \$10,000 for each violation
10 of California Penal Code § 593e. In addition, award Plaintiffs \$50,000 for each
11 knowing and willful violation of § 593e committed for purposes of commercial
12 advantage or private financial gain, plus punitive damages.

13 O. In accordance with California state law, Order an accounting, establish a
14 constructive trust in favor of Plaintiffs, and direct Defendants to make restitution as
15 a result of: (a) designing, manufacturing, assembling, modifying, importing (to the
16 United States), trafficking, possessing, distributing, or selling Pirated EchoStar
17 Access Cards or other Circumvention or Signal Theft Technology and Devices; (b)
18 providing software, information, or technical support services relating to: (1)
19 altering, pirating, modifying, compromising, and/or counterfeiting EchoStar Access
20 Cards; (2) Pirated EchoStar Access Cards; (3) other Circumvention or Signal Theft
21 Technology or Devices; or (4) the illegal and unauthorized reception and use of
22 EchoStar's satellite television Programming services by persons not authorized to
23 receive such programming; (c) assisting, procuring, or aiding and abetting third
24 persons in the unauthorized reception and use of EchoStar's satellite television
25 Programming services; or (d) advertising the sale of Pirated EchoStar Access Cards
26 or other Circumvention or Signal Theft Devices;

27 P. In accordance with 17 U.S.C. § 1203(b)(4)-(5), 47 U.S.C. § 605(e)(3)(B)(iii),
28 18 U.S.C. § 1964(c), California Penal Code § 593d(f), and California Penal Code §

1 593e(d) direct Defendants to pay Plaintiffs all of Plaintiffs' costs, reasonable
2 attorneys' fees, and investigative fees;

3 Q. For pre-judgment interest on all damages, where allowable by law;

4 R. For post-judgment interest on all damages, where allowable by law; and

5 S. For such additional relief as the Court deems to be just and equitable.

6

7

PLAINTIFFS' DEMAND FOR JURY TRIAL

8 Plaintiffs hereby assert their rights under the Seventh Amendment to the
9 United States Constitution and demand, in accordance with FRCP 38, a trial by jury
10 on all issues excepting equitable/injunctive relief specifically sought above.

11

12 DATED: January 31, 2008

13

Respectfully submitted,

14

T. WADE WELCH & ASSOCIATES

15

16

By: 

Chad M. Hagan (*pro hac vice*)

2401 Fountainview, Suite 700

Houston, Texas 77057

Telephone: (713) 952-4334

Facsimile: (713) 952-4994

20

21

Attorneys for Plaintiffs

EchoStar Satellite LLC, *et al*

22

23

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

Additional Counsel:

DLA PIPER US LLP

Cynthia A. Ricketts (*pro hac vice*)
David A. Grenardo (State Bar No. 223142)
1999 Avenue of the Stars, Fourth Floor
Los Angeles, California 90067
Telephone: (310) 595-3000
Facsimile: (310) 595-3300