

1 SQUIRE, SANDERS & DEMPSEY L.L.P.
Cynthia A. Ricketts (*pro hac vice*)
2 Michael T. Purliski (State Bar No. 216307)
801 S. Figueroa St., Fourteenth Floor
3 Los Angeles, California 90017
Telephone: (213) 624-2500
4 Facsimile: (213) 623-4581

COPY

5 T. WADE WELCH & ASSOCIATES
T. Wade Welch (*pro hac vice*)
6 Ross W. Wooten (*pro hac vice*)
Chad M. Hagan (*pro hac vice to be filed*)
7 2401 Fountainview, Suite 700
Houston, Texas 77057
8 Telephone: (713) 952-4334
Facsimile: (713) 952-4994

NOT IN CONTROL

9 Attorneys for Plaintiffs
10 ECHOSTAR SATELLITE
CORPORATION,
11 ECHOSTAR COMMUNICATIONS
CORPORATION, ECHOSTAR
12 TECHNOLOGIES
CORPORATION, AND NAGRASTAR,
13 L.L.C.

14 UNITED STATES DISTRICT COURT
15 CENTRAL DISTRICT OF CALIFORNIA
16 SOUTHERN DIVISION

17 ECHOSTAR SATELLITE
CORPORATION, ECHOSTAR
18 COMMUNICATIONS
CORPORATION, ECHOSTAR
19 TECHNOLOGIES
CORPORATION, AND
20 NAGRASTAR L.L.C.

21 Plaintiffs,

22 v.

23 NDS GROUP PLC, NDS
AMERICAS, INC., JOHN
24 NORRIS, REUVEN HASAK,
OLIVER KOMMERLING,
25 JOHN LUYANDO, PLAMEN
DONEV, VESSELINA
26 NEDELICHEV,
CHRISTOPHER TARNOVSKY,
27 ALLEN MENARD, LINDA
WILSON, MERVIN MAIN,
28 DAVE DAWSON, SHAWN

No. SA CV 03-950 DOC(ANx)
**PLAINTIFFS' SECOND AMENDED
COMPLAINT FOR:**

- 1) **Violation of the Digital
Millennium Copyright Act, 17
U.S.C. § 1201(a)(1)(A);**
- 2) **Violation of the Digital
Millennium Copyright Act, 17
U.S.C. § 1201(a)(2);**
- 3) **Violation of the Digital
Millennium Copyright Act, 17
U.S.C. § 1201(b);**
- 4) **Violation of the Communications
Act of 1934, as amended, 47
U.S.C. § 605(a);**
- 5) **Violation of the Communications
Act of 1934, as amended, 47
U.S.C. § 605(e)(4);**

1 QUINN, ANDRE SERGEI,
2 TODD DALE, STANLEY
3 FROST, GEORGE
4 TARNOVSKY, BRIAN
5 SOMMERFIELD, ED BRUCE,
6 "BEAVIS," "JAZZERCZ,"
7 "STUNTGUY," and JOHN
8 DOES 1 – 10C.

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

- 6) Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)(a);
- 7) Violation of the Lanham Act, 15 U.S.C. § 1114;
- 8) Violation of the Lanham Act, 15 U.S.C. § 1125(a);
- 9) Violation of RICO Statute, 18 U.S.C. § 1962(c);
- 10) Violation of RICO Statute, 18 U.S.C. § 1962(d)
- 11) Violation of California Penal Code §§ 593d(a);
- 12) Violation of California Penal Code § 593d(b);
- 13) Violation of California Penal Code § 593d(c);
- 14) Violation of California Penal Code § 593e(a);
- 15) Violation of California Penal Code § 593e(b);
- 16) Unfair Competition in Violation of California Business & Professions Code § 17200;
- 17) Tortious Interference with Contractual Relations;
- 18) Tortious Interference with Prospective Contractual Relations/Economic Advantage;
- 19) Unjust Enrichment;
- 20) Conversion;
- 21) Negligent Hiring, Training, Supervision and/or Retention;
- 22) Breach of Contract;
- 23) Civil Conspiracy.

JURY TRIAL DEMANDED

1 Plaintiffs EchoStar Communications Corporation, EchoStar Satellite L.L.C.
2 f/k/a EchoStar Satellite Corporation, and EchoStar Technologies Corporation
3 (collectively "EchoStar") and NagraStar L.L.C. ("NagraStar") (collectively
4 "Plaintiffs") file their Second Amended Complaint against the above named
5 Defendants and state as follows.

6 **I. INTRODUCTION & NATURE OF THE CASE**

7 1. Plaintiff EchoStar is a multi-channel video provider, providing video,
8 audio, and data services to customers throughout the United States, Puerto Rico,
9 and the U.S. Virgin Islands via a Direct Broadcast Satellite ("DBS") system. As
10 part of its business, EchoStar uses high-powered satellites to broadcast, among
11 other things, movies, sports, and general entertainment programming services
12 ("Programming") to consumers who have been legally authorized to receive its
13 Programming after payment of a subscription fee (or in the case of a pay-per-view
14 movie or event, the purchase price). EchoStar operates its DBS Programming
15 service under the trade name "DISH Network" which was launched in 1996.

16 2. In order to protect its signal from unlawful and unauthorized use, a
17 DBS provider must encrypt its satellite signal. EchoStar encrypts its satellite
18 signals using a technology provided, in part, by NagraStar. NagraStar is a supplier
19 of access cards or "smart cards" ("Smart Card") which contain tiny microprocessors
20 embedded therein and which facilitate functions of a larger "conditional access
21 system" ("CAS") known as Digital Nagra Advanced Security Process ("DNASP").
22 DNASP uses a complex encryption system that is combined with a Digital Video
23 Broadcasting ("DVB") scrambler/encoder system to form EchoStar's management
24 and Security System ("Security System"). Among other things, the Security System
25 serves two interrelated functions: (1) subscriber management – allowing EchoStar
26 to "turn on" programming that a customer has ordered; and (2) encryption –
27 preventing individuals or entities who have not ordered programming from
28 receiving it.

1 3. Defendants NDS and NDS Americas (“NDS”) are the only major
2 competitor of Plaintiff NagraStar in the CAS marketplace. NDS provides the
3 encryption technology used by DirecTV. DirecTV is Plaintiff EchoStar’s only
4 major competitor in the DBS industry.

5 4. In or around 1998, NDS was involved in efforts to convince EchoStar
6 to switch CAS providers from NagraStar to NDS. These efforts were ultimately
7 unsuccessful, however, because at that time the CAS provided to EchoStar by
8 NagraStar had never been compromised. Conversely, the NDS system used by
9 DirecTV was widely hacked and pirated resulting in an exponentially increasing
10 number of satellite pirates having the ability to receive DirecTV’s satellite
11 programming without an authorized subscription and without proper payment to
12 DirecTV. During this same time period, NDS was experiencing similar problems
13 with the customers it provided CAS services to in Europe as well.

14 5. Ultimately, NDS’s inability to provide a secure CAS product to its
15 customers resulted in a total loss of confidence in NDS’s encryption technology. In
16 fact, the satellite piracy and hacking of DirecTV’s signal became so uncontrollable
17 that, in 1998, DirecTV began to solicit proposals from other CAS providers in the
18 industry.

19 6. The leading candidate for DirecTV’s solicitation was the CAS
20 provided by NagraStar to EchoStar. DirecTV was so dissatisfied with NDS’s
21 product that it paid NagraStar \$100,000 to devise a proposal and bid for contracting
22 with DirecTV to be its new CAS provider.

23 7. In sum, NDS was on the verge of losing one of its largest accounts,
24 DirecTV, and ultimately, its ability to effectively compete in the CAS industry.
25 Indeed, NDS internal documents cited herein are illustrative of NDS’s knowledge
26 of the vulnerability¹ of its conditional access system, the real and immediate threat

27 ¹ September 26, 1997 NDS Memorandum Report to Hasak stating “At present I think we are on
28 the edge of a serious situation...part of the problem is the history of the insecurity of our
technology...we must face the fact that our reputation is bad and our competitors make capital out

1 of losings its clients (e.g., DirecTV) to its competitors, such as NagraStar, and that
2 high level executives in charge of NDS's security division had their "jobs in
3 jeopardy." NDS knew it needed to act, and act quickly, if it was to have any chance
4 of commercial survival.

5 8. However, instead of making advancements in its technology and
6 improving its product in order to fairly and legally compete in the marketplace,
7 NDS made the calculated decision to hire the "worst" and most well-known
8 satellite pirates and hackers in the world in an effort to establish and maintain
9 "CONTROL" over the compromising of its CAS product as well as its competitors'
10 technology. NDS concluded that if it could "CONTROL" the hackers and the
11 constant breaks into its security system, as well as orchestrating breaks into its
12 competitors' security systems, then NDS's product would appear superior in the
13 market place.²

14 9. In order to implement this plan, NDS first had to get "CONTROL"
15 over the hacks and piracy of its own clients, such as DirecTV. To accomplish this,
16 NDS launched a massive attack on the satellite pirates in the United States and
17 Canada that were responsible for compromising the CAS that NDS provided to
18 DirecTV. Accordingly, NDS offered its resources and assistance to various law
19 enforcement agencies to initiate criminal proceedings, as well as attacking these
20 same pirates on the civil front by filing numerous civil suits.

21
22 of it...We have introduced control. The question is whether the control is camouflaging the
23 weaknesses in our technology. My fear is that it is....At present we are not gaining most of the
24 new projects. How long before we actually lose one to a competitor. Our jobs are on the line.
25 Maybe not yet but we are vulnerable." June 18, 1999 NDS Letter to Hasak from Adams stating
26 "JOD was heavily involved in the DTV negotiations. He thinks we will lose them soon. We will
27 lose them quicker if P3 is hacked. This must be a major concern."

28 ² December 1998 NDS Letter is from Ray Adams to Hasak stating "It should be a simple task for
one of our techies to prove that the Austrailian Irdeto card is as vulnerable [hack the card] as any
in any other country...What we [NDS] need urgently are some official cards from each of the
systems, six of each, making 18 total so that we can get the pirates to switch them on. This is the
easiest way to prove our case. It will also be very effective and untraceable."

1 10. Once NDS was able to put enough legal pressure on the pirating
2 community, it began to recruit the hackers responsible for compromising NDS's
3 technology and put them on the NDS payroll.³ Specifically, from as early as 1998,
4 NDS employed, protected, paid, and controlled well-known satellite hackers and
5 pirates including, but not limited to, Christopher Tarnovsky, Oliver Kommerling,
6 Plamen Donev, Vesseline Nedeltchev, Jan Saggiori, Dieter Scheel, and John
7 Luyando. With these notorious hackers on their payroll, and acting under the
8 protective umbrella NDS provided to them, NDS was now able to "CONTROL"
9 the piracy of its clients like DirecTV. With this "CONTROL" of the hackers, NDS
10 was also able to gain the ability to put economic leverage on its clients.
11 Specifically, NDS could instruct, assist, and/or otherwise facilitate these hacker
12 employees in pirating a client's CAS. Once compromised, NDS could offer the
13 client – **for a fee** - an Electronic Counter Measure ("ECM") that would combat the
14 hack which, unbeknownst to the client, NDS was controlling. Accordingly, Phase 1
15 of the NDS plan to conquer the CAS market was complete.

16 11. Phase 2 of the NDS scheme involved NDS gaining the ability to
17 "CONTROL" the piracy of its competitors' security systems. In order to
18 accomplish this goal, NDS took a four (4) step approach.

19 12. Step 1 required NDS to obtain the Read Only Memory ("ROM") and
20 Electronically Erasable Programmable Read Only Memory ("EEPROM") Codes
21 used in their competitors' Smart Cards. These proprietary codes form the heart and
22 soul of CAS providers' security system and, as such, are secured and embedded in
23 the tiny microprocessor unit stored in the Smart Card. To extract these codes, NDS
24 needed a state-of-the-art laboratory, extremely sophisticated equipment like a
25 scanning electron microscope and focused ion beam, and highly skilled engineers.
26 There are only approximately six (6) of these labs in the world – NDS owns one of

27 ³ Additionally, Plaintiffs are informed and believe that some of these pirates (e.g., Tarnovsky)
28 were paid through other companies such as HarperCollins Publishers in New York, which are
linked to NDS's parent company, News Corp.

1 them in Haifa, Israel, which was designed and built by NDS with the assistance of
2 Kommerling⁴ and used by NDS to extract the ROM and EEPROM codes utilized
3 by NDS's competitors.

4 13. Using its Haifa laboratory, NDS unlawfully and impermissibly cracked
5 Plaintiffs' Smart Card and extracted Plaintiffs' secret ROM and EEPROM Codes
6 secured therein. This was not the first time NDS engaged in this unlawful conduct.⁵
7 On April 9, 2002, NDS employee/agent Kommerling provided sworn testimony in
8 another suit⁶ brought by Canal+ against NDS for anticompetitive conduct similar to
9 the acts alleged herein. In his declaration, Kommerling explained the methods
10 NDS used to break the security system of Canal+ and to subsequently distribute
11 that information to foster the satellite piracy of the Canal+ system.

12 14. Step 2 involved NDS transferring these unlawfully extracted ROM and
13 EEPROM Codes to a pirating software engineer capable of using the Codes to
14 unlawfully access, reprogram, modify, alter, or otherwise interfere with the Smart
15 Cards used by Plaintiffs to protect the DISH Network satellite signal. NDS
16 accomplished this task by using one of its new hacker recruits, Chris Tarnovsky,
17 who had previously been responsible for compromising the CAS provided by NDS
18 to DirecTV. NDS had recently moved Tarnovsky to California. Accordingly, NDS

19 ⁴ In 1999, Kommerling and Markus Kuhn co-wrote "Design Principles for Tamper Resistant Smart
20 Cards." This publication became the standard text on how to "reverse engineer" a state-of-the-art
21 smartcard by using certain techniques including, but not limited to, acid treatments, microscopic
22 probes, laser cutting, and ion beam manipulation.

23 ⁵ April 30, 1999 NDS Letter from Ray Adams to Hasak referencing a meeting that Kommerling
24 had with Canal+, wherein Kommerling was asked about the DR7 [Menard] Hack release.
25 Kommerling was asked if he could do a hack of the IRDeto system in Arabia on PANAM SAT
26 channel ART 1, however, unbeknownst to Canal+, the hack of IRDeto was already in NDS's
27 possession. "JR wants Alex [Kommerling] to hack the system but at the same time to provide a
28 fix. So that when the pirate cards are available he will be able to say that Alex 'the technician' can
do a fix in 24 hours. . . . What JR does not know is that the hack is already in our [NDS's]
possession.

⁶ Plaintiffs first attempted to assert their claims against NDS by moving to intervene in the
Canal+ v. NDS litigation. Not surprisingly, NDS fought vigorously to keep Plaintiffs' Motion to
Intervene from being heard or ruled upon. Ultimately, NDS settled with Canal+ prior to
Plaintiffs' Motion to Intervene being considered by the Court. Accordingly, Plaintiffs filed the
instant action.

1 transmitted Plaintiffs' ROM and EEPROM Codes to Tarnovsky via Reuven Hasak
2 (Israel) and John Norris (California), both of which were/are NDS employees.
3 Tarnovsky has previously admitted to Kommerling that NDS provided Tarnovsky
4 with Plaintiffs' ROM and EEPROM Codes via Hasak and Norris. In a similar vein,
5 on or about October 5, 2001, Tarnovsky also admitted to Gilles Kaehlin, Head of
6 Security for Canal+, that NDS was behind the Canal+ hack and that NDS provided
7 Tarnovsky with the full Canal+ ROM code via Hasak and Norris.

8 15. At the direction and under the control of NDS, and with assistance
9 provided by NDS, Tarnovsky was able to use Plaintiffs' Codes to design and build
10 a pirating device that was capable of reprogramming Plaintiffs' smart cards thereby
11 allowing others to gain unauthorized and unlawful access to Plaintiffs' satellite
12 programming. NDS and Tarnovsky named this reprogrammer "the stinger."

13 16. Step 3 involved NDS distributing these illegally reprogrammed and
14 pirated EchoStar smart cards to the pirating community in a "CONTROLLED"
15 manner.⁷ To accomplish this, NDS, via Tarnovsky, enlisted the assistance of Allen
16 Menard⁸ and his hacker website, www.dr7.com. With the assistance of NDS and
17 Tarnovsky, Menard set up a "CONTROLLED" distribution network consisting of a
18 limited number of dealers through which NDS and Tarnovsky could traffic and
19 distribute the reprogrammed and pirated EchoStar Smart Cards. Through these
20 distribution dealers – Dave Dawson, Shawn Quinn, Andre Sergei, Todd Dale, and
21 Stanley Frost, among others – NDS, Tarnovsky, and Menard could "CONTROL"
22 the number of pirated EchoStar Smart Cards that were distributed to the pirating
23 public.

24 ⁷ It was during the early stages of Step 3 that NDS informed DirecTV that the CAS provider
25 DirecTV was considering switching to (i.e., Plaintiffs' system) in lieu of the NDS system it was
26 currently using, had been compromised. Based on this, DirecTV renewed its contract with NDS
as their CAS provider.

27 ⁸ April 16, 1999 NDS Letter from Ray Adams to Hasak concerning, among other things, a piracy
28 investigation of www.dr7.com and "DR7" [Menard]. Adams states, "[s]omewhere in the loop
appears PINKERTON investigative Service. They at one time worked for Irdeto as well as other
companies. There is talk that an agency is investigating DR7[Menard]."

1 17. In addition to Dawson, Quinn, Sergei, Dale, and Frost, among others,
2 Menard and Tarnovsky approached other individuals to help facilitate and promote
3 the overriding NDS conspiracy. Specifically, in April 1999 and then again in
4 November 1999, Menard approached Reginald Scullion with an offer to participate
5 in the “DISH Network” hack. During these conversations, Menard informed
6 Scullion that, among other things: (a) NDS was behind the EchoStar hack; (b) the
7 Tarnovsky/Menard distribution model would be protected and controlled by NDS;
8 (c) NDS had an arrangement with Tarnovsky to provide the technical and software
9 support and facilitate the hacked EchoStar ROM Code to be sent to Menard and
10 used in the distribution network; and (d) NDS would protect this distribution
11 network from potential RCMP raids.

12 18. NDS and Tarnovsky were able control the distribution of these pirated
13 smart cards because the “stinger” developed by NDS and Tarnovsky, and
14 subsequently provided to Menard, would only reprogram a predetermined number
15 of cards before it would lock up. At that point, Menard would send cash payments
16 to Tarnovsky in California, via a forwarding mailbox Tarnovsky set up in Texas,
17 which was concealed inside of various consumer electronic products (*e.g.*, CD and
18 DVD players).⁹ Once Tarnovsky received these payments, he would write a
19 program which would reactivate the “stinger” until the card number had been
20 reached again. NDS, Tarnovsky, and Menard continued with this method of
21 controlled distribution for over a year. Through this method, NDS and Tarnovsky
22 were able to effectively “CONTROL” the piracy of Plaintiffs’ Security System
23 because they were the *only ones* capable of reprogramming or “pirating” an
24

25 _____
26 ⁹ Eventually, the method of payments from Menard to NDS and Tarnovsky was discovered by
27 U.S. Customs officials who launched an investigation into Tarnovsky’s activities of satellite
28 piracy and money laundering. Notably, when this investigation lead to a raid on Tarnovsky’s
California home in 2001 NDS executive John Norris immediately informed Customs’ officials
that Tarnovsky was an NDS employee, all the equipment [used for satellite piracy] in
Tarnovsky’s home belonged to NDS, and officials were not to question Tarnovsky or search
Tarnovsky’s home without NDS’s counsel being present.

1 EchoStar Smart Card – such reprogramming being accomplished via NDS and
2 Tarnovsky’s “stinger.”

3 19. Step 4 involved NDS releasing the necessary instructions and
4 procedures necessary to obtain Plaintiffs’ ROM and EEPROM Codes directly to the
5 pirating community in an effort to destroy NDS’s only viable competitor. Up until
6 this point, NDS concealed Plaintiffs’ proprietary information from the hacking
7 public in furtherance of the NDS objective to “CONTROL” the piracy of Plaintiffs’
8 Security System. However, during the period when NDS, Tarnovsky, and Menard
9 operated the monopoly of the piracy of Plaintiffs’ Security System, Plaintiffs began
10 to engage in countermeasures to combat their piracy problem. Specifically,
11 Plaintiffs employed various Electronic Counter Measures (ECMs) in attempts to
12 disable the pirated Smart Cards that were being provided by NDS, via Tarnovsky
13 and Menard.

14 20. As evidenced by a significant number of chat posts cited herein, the
15 end user pirates obtaining reprogrammed EchoStar Smart Cards from NDS, via
16 Tarnovsky and Menard, became discontent with the inability of these pirated Smart
17 Cards to withstand Plaintiffs’ ECMs. Specifically, with the “CONTROLLED”
18 distribution network designed and implemented by, among others, NDS,
19 Tarnovsky, and Menard, end users who purchased one of these reprogrammed
20 EchoStar Smart Cards would have to send them back to Menard/Tarnovsky, either
21 directly or through dealers Dawson, Quinn, Sergei, Dale, and Frost, among others,
22 for “fixes” or “updates” each time Plaintiffs launched an ECM to disable the pirated
23 Smart Cards. Eventually, the NDS, Tarnovsky, and Menard “CONTROLLED”
24 distribution network was unable to effectively keep up with the ECMs employed by
25 Plaintiffs to disable the pirated EchoStar Smart Cards being reprogrammed,
26 marketed and distributed by Defendants. Additionally, as NDS, Tarnovsky, and
27 Menard had already made an obscene amount of illegal revenue through the
28 trafficking of these pirated Smart Cards, NDS “pulled the trigger” on Step 4 of their

1 overriding conspiracy to destroy Plaintiffs as a competitors in the DBS and CAS
2 marketplaces.

3 21. Indeed, on December 23 and 24, 2000, NDS effectuated and assisted
4 others in effectuating a wide spread compromise of Plaintiffs' conditional access
5 system. On these dates, using the nickname "nIpPeR¹⁰ cLaUz 00'," among others,
6 and under the direction and control of NDS, and with NDS's full knowledge and
7 ratification, Tarnovsky posted a sequence of events and data, along with
8 accompanying instructional code, that provided satellite pirates around the world
9 the "road map" and requisite instructions for the full dump of Plaintiffs' secret
10 EEPROM Code. Tarnovsky posted the foregoing, which was illegally obtained by
11 NDS in its Haifa, Israel lab and sent to Tarnovsky in California, via Hasak and
12 Norris, with the specific instructions to effectuate and assist others in effectuating a
13 wide spread compromise of Plaintiffs' conditional access system, on the Internet
14 website www.piratesden.com. In addition to allowing these satellite pirates to
15 procure the full dump of Plaintiffs' EEPROM Code, the December 23 and 24, 2000
16 postings and assistance provided by NDS, Tarnovsky, and Menard, among others,
17 also allowed these same hackers to readily procure a full dump of Plaintiffs' secret
18 ROM Code. With this assistance, satellite pirates around the world now had all the
19 requisite proprietary information that was once secured in Plaintiffs'
20 microprocessor. Specifically, with this December 23 and 24, 2000 assistance by
21 NDS, Tarnovsky, and Menard, among others, satellite pirates were then able to
22 build their own card reprogrammers and, thus, were able to break free from their
23 dependence on NDS, Tarnovsky and Menard, among others, for obtaining
24 reprogrammed EchoStar Smart Cards. Consequently, NDS's goal of effectuating

25 ¹⁰ The name "NiPpEr" used by Tarnovsky to post Plaintiffs' proprietary information is
26 significant. Specifically, when Plaintiffs' Security System was developed, NagraStar's engineers
27 concealed the term "NiPpEr" in the very heart of the secret ROM Code to serve as a unique
28 identifier for Plaintiffs' Code. Accordingly, when Tarnovsky used this name when providing the
detailed instructions on how to fully dump Plaintiffs' secret EEPROM and ROM Codes, he was
revealing to Plaintiffs that he had in fact already seen Plaintiffs' secret codes which were
transmitted to him from NDS's Haifa facility to Tarnovsky in California via Hasak and Norris.

1 and assisting others in effectuating the widespread compromise of Plaintiffs'
2 Security System began to rapidly materialize.

3 22. As a result of the conduct alleged herein, particularly the December
4 23 and 24, 2000 postings by Tarnovsky with the assistance and direction of NDS,
5 Plaintiffs have suffered and will continue to suffer substantial damages.
6 Particularly, *the December 23 and 24, 2000 postings by NDS/Tarnovsky put at risk*
7 *over 7.6 million of Plaintiffs' Smart Cards already distributed in the marketplace.*
8 *Consequently, Step 4 of the NDS conspiracy rendered a global card-swap by*
9 *Plaintiffs unavoidable.*

10 23. The anticompetitive method in which NDS conspired to, and did,
11 launch an invasive attack on Plaintiffs' conditional access system and subsequently
12 design and implement the widespread compromise of Plaintiffs' Security System
13 shocks the conscience of modern-day capitalism and basic tenets of lawful
14 competition. The unlawful acts engaged in by Defendants in furtherance of the
15 overriding NDS conspiracy form the backdrop of an unprecedented level of
16 corporate espionage and are illustrative of nothing less than high risk corporate
17 financed organized crime. The time has finally come for NDS to answer for its
18 actions.

19 **II. JURISDICTION & VENUE**

20 24. Jurisdiction and venue are proper in this court. This Court has original
21 federal question subject matter jurisdiction over this action under 28 U.S.C. §§
22 1331 and 1338, the Communications Act of 1934, as amended, 47 U.S.C. §
23 605(e)(3)(A), the Digital Millennium Copyright Act, 17 U.S.C. § 1203, the
24 Electronic Communications Privacy Act ("Federal Wiretap Laws"), 18 U.S.C.
25 §2520(a), the Lanham Trademark Act, 15 U.S.C. §§ 1051 *et seq.*, the Racketeer
26 Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1965(b), and 15
27 U.S.C. § 1121(a). Alternatively, this Court has subject matter jurisdiction of this
28 action under 28 U.S.C. § 1332(a)(1) by virtue of the complete diversity of

1 citizenship of the parties in an action in which the matter in controversy exceeds the
2 sum or value of \$75,000, exclusive of interest and costs. This Court also has
3 supplemental jurisdiction, pursuant to 28 U.S.C. 1367(a), over the California state
4 law claims asserted herein.

5 25. Personal jurisdiction and venue are proper in this judicial district
6 pursuant to 28 U.S.C. §§ 1391(b), (c), and (d), 18 U.S.C. § 1965(a), (b), and (d),
7 and Federal Rule of Civil Procedure 4(k)(1) and (2). Pursuant to 18 U.S.C. § 1965,
8 Plaintiffs allege that (1) Defendants have engaged in a multi-district conspiracy, (2)
9 this Court has personal jurisdiction of at least one participant, and (3) there is no
10 other District in which the United States District Court would have personal
11 jurisdiction over all the co-conspirators. In addition the Alien Venue Act, 28 U.S.C.
12 Section 1391(d) provides that “an alien may be sued in any district.” Venue is
13 additionally proper in this District and all Defendants named herein are subject to *in*
14 *personam* jurisdiction in this District because each Defendant has made repeated
15 and substantial contacts with this judicial district by, *inter alia*, providing assistance
16 to NDS and/or Tarnovsky in this District in serving their role in the overriding NDS
17 conspiracy to effectuate and facilitate others in effectuating a wide spread
18 compromise of Plaintiffs’ conditional access system. Further, venue is proper in
19 this District because a substantial part of the events giving rise to Plaintiffs’ claims.
20 Defendants have further advertised, solicited orders from and/or sent satellite
21 pirating equipment and/or proceeds unlawfully obtained through the trafficking in
22 satellite pirating equipment through interstate commerce to this State.

23 **III. PARTIES & RELATIONSHIP TO PLAINTIFFS’ SUIT**

24 26. Plaintiff EchoStar Communications Corporation (“ECC”) is a Nevada
25 corporation with its principal place of business at 5701 S. Santa Fe, Littleton,
26 Colorado 80120. ECC is the corporate parent of EchoStar Satellite Corporation and
27 EchoStar Technologies Corporation, and is a fifty-percent owner of NagraStar
28 L.L.C.

1 27. Plaintiff EchoStar Satellite L.L.C., (“ES”) f/k/a EchoStar Satellite
2 Corporation, is a Colorado corporation with its principal place of business at 5701
3 S. Santa Fe, Littleton, Colorado 80120.

4 28. Plaintiff EchoStar Technologies Corporation (ETC”) is a Texas
5 corporation that is a wholly owned subsidiary of ECC. Plaintiff ETC has its
6 principal place of business at 90 Inverness Circle East, Englewood, Colorado
7 80112.

8 29. Plaintiff NagraStar L.L.C. (“NagraStar”) is a joint venture and
9 Colorado corporation with its principal place of business at 90 Inverness Circle
10 East, Englewood, Colorado 80112.

11 30. Defendant NDS Group, PLC (“NDS Group”) is incorporated under the
12 laws of England and Wales, with its registered address for service at One London
13 Road, Staines, Middlesex, England TW18 4EX and its U.S. agent for service of
14 process is Arthur Siskind c/o The News Corporation Limited, 1211 Avenue of the
15 Americas, New York, New York.

16 31. Upon information and belief Defendant NDS Group is still currently
17 in possession of: (a) Plaintiffs’ proprietary information including but not limited to
18 proprietary sections of Plaintiffs’ ROM code, Plaintiffs’ EEPROM code, and/or
19 other proprietary information unlawfully extracted from the microprocessor
20 embedded in Plaintiffs’ Access ‘Smart’ Cards; (b) software, hardware, Pirated
21 EchoStar Access Cards and/or other circumvention or signal theft devices designed
22 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’
23 Security System (including, but not limited to, loaders, dead processor boot boards,
24 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
25 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,
26 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
27 for the unlawful and unauthorized modification of and/or access to EchoStar’s
28 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained

1 through the sale/distribution of, or assistance or support provided in connection
2 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
3 signal theft devices designed to enable users to illegally modify or alter EchoStar
4 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
5 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
6 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
7 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
8 other hardware and software intended for the unlawful and unauthorized
9 modification of and/or access to EchoStar's digital satellite system).

10 32. Defendant NDS Americas, Inc. ("NDS Americas") is a Delaware
11 Corporation with its principal place of business in Newport Beach, California, and
12 its registered agent for service of process is John Workman, 3501 Jamboree Road,
13 Suite 200, Newport Beach, California.

14 33. Upon information and belief Defendant NDS Americas is still
15 currently in possession of: (a) Plaintiffs' proprietary information including but not
16 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
17 and/or other proprietary information unlawfully extracted from the microprocessor
18 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
19 EchoStar Access Cards and/or other circumvention or signal theft devices designed
20 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
21 Security System (including, but not limited to, loaders, dead processor boot boards,
22 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
23 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
24 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
25 for the unlawful and unauthorized modification of and/or access to EchoStar's
26 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
27 through the sale/distribution of, or assistance or support provided in connection
28 with, among others, Pirated EchoStar Access Cards and/or other circumvention or

1 signal theft devices designed to enable users to illegally modify or alter EchoStar
2 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
3 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
4 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
5 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
6 other hardware and software intended for the unlawful and unauthorized
7 modification of and/or access to EchoStar's digital satellite system).

8 34. Defendant John Norris a/k/a "JN" ("Norris") is an individual and
9 citizen of the United States, residing in California, who was employed by NDS at
10 all relevant times stated herein. During all times relevant as stated herein, Norris
11 was either: (a) working for, at the direction of, and under the direct and/or indirect
12 control of NDS, and with NDS's full knowledge and/or ratification, as well as for
13 his own individual interest and/or gain, as a participant in the overriding NDS
14 conspiracy to effectuate and/or facilitate others in effectuating a wide spread
15 compromise of Plaintiffs' conditional access system; or (b) working in concert with
16 NDS, its employees and/or agents in serving his role in the overriding NDS
17 conspiracy to effectuate and facilitate others in effectuating a wide-spread
18 compromise of Plaintiffs' conditional access system.

19 35. Upon information and belief John Norris is still currently in
20 possession of: (a) Plaintiffs' proprietary information including but not limited to
21 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
22 other proprietary information unlawfully extracted from the microprocessor
23 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
24 EchoStar Access Cards and/or other circumvention or signal theft devices designed
25 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
26 Security System (including, but not limited to, loaders, dead processor boot boards,
27 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
28 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,

1 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
2 for the unlawful and unauthorized modification of and/or access to EchoStar's
3 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
4 through the sale/distribution of, or assistance or support provided in connection
5 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
6 signal theft devices designed to enable users to illegally modify or alter EchoStar
7 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
8 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
9 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
10 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
11 other hardware and software intended for the unlawful and unauthorized
12 modification of and/or access to EchoStar's digital satellite system).

13 36. Norris is the Vice President of Special Projects for NDS Americas,
14 Inc. and is the Head of Security for NDS North America. Norris recruited and hired
15 satellite hackers Christopher Tarnovsky ("Tarnovsky"), Oliver Kommerling
16 ("Kommerling"), Plamen Donev ("Donev"), and Vesselin Nedeltchev
17 ("Nedeltchev"), among others, for Rupert Murdoch, in or about 1997, for the
18 purpose of gaining intelligence in the pirate world and to control them due to their
19 impact on NDS's vulnerable market position in conditional access technology.
20 From approximately 1997 to present date, Norris has maintained close relationships
21 with all of the satellite hackers recruited and hired by NDS, specifically Tarnovsky
22 and Kommerling.

23 37. Plaintiffs are informed and believe that Norris, Tarnovsky, and Hasak
24 attended a meeting on or about 1999 whereby the full DISH Network secret ROM
25 and EEPROM codes were given to Tarnovsky. The origination of the hack of the
26 full DISH Network secret ROM and EEPROM codes was at NDS's Matam
27 laboratory located in Haifa, Israel.

28

1 38. On February 9, 2001, U.S. Customs officials raided Tarnovsky's
2 California residence based on information and evidence obtained by them during an
3 investigation of Tarnovsky's involvement with satellite piracy and money
4 laundering. Shortly after entry of Tarnovsky's residence, Norris informed U.S.
5 Customs officials that (1) Tarnovsky was, in fact, a NDS employee, (2) all property
6 located at Tarnovsky's California residence belonged to and was NDS's property,
7 and (3) U.S. Customs officials were not permitted to search Tarnovsky's California
8 residence or speak to Tarnovsky without NDS's counsel present.

9 39. Defendant Reuven Hasak a/k/a "RH" ("Hasak") is an individual and
10 citizen of Israel, residing in Israel. During all times relevant as stated herein,
11 Hasak was either: (a) working for, at the direction of, and under the direct and/or
12 indirect control of NDS, and with NDS's full knowledge and/or ratification, as
13 well as for his own individual interest and/or gain, as a participant in the overriding
14 NDS conspiracy to effectuate and/or facilitate others in effectuating a wide spread
15 compromise of Plaintiffs' conditional access system; or (b) working in concert with
16 NDS, its employees and/or agents in serving his role in the overriding NDS
17 conspiracy to effectuate and facilitate others in effectuating a wide-spread
18 compromise of Plaintiffs' conditional access system.

19 40. Upon information and belief Defendant Reuven Hasak is still
20 currently in possession of: (a) Plaintiffs' proprietary information including but not
21 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
22 and/or other proprietary information unlawfully extracted from the microprocessor
23 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
24 EchoStar Access Cards and/or other circumvention or signal theft devices designed
25 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
26 Security System (including, but not limited to, loaders, dead processor boot boards,
27 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
28 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,

1 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
2 for the unlawful and unauthorized modification of and/or access to EchoStar's
3 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
4 through the sale/distribution of, or assistance or support provided in connection
5 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
6 signal theft devices designed to enable users to illegally modify or alter EchoStar
7 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
8 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
9 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
10 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
11 other hardware and software intended for the unlawful and unauthorized
12 modification of and/or access to EchoStar's digital satellite system).

13 41. Hasak is Head of Security for NDS in Haifa, Israel. Hasak is a former
14 deputy of the Shin Bet, the Israeli internal security service. Hasak is fully aware of
15 NDS's problems associated with the conditional access technology of its security
16 system in that it is insecure and easily hacked. Hasak is fully aware of NDS's
17 efforts and plan to "CONTROL" satellite piracy by recruiting and hiring known
18 satellite pirates to work as double agents on NDS assignments. Hasak, Norris,
19 Adams, Gutman, and Segoli conspired with the satellite pirates NDS hired
20 including, but not limited to, Tarnovsky, Kommerling, Donev, and Nedeltchev,
21 among others, to (1) illegally obtain and extract NDS's competitors' ROM codes
22 and keys, (2) illegally design, manufacture, and distribute signal theft devices used
23 to circumvent the technological encryption measures contained in satellite
24 providers' access cards for the unauthorized reception of satellite television
25 programming, (3) illegally provide software, information, and technical support
26 services relating to satellite providers' access cards and other circumvention or
27 signal theft devices designed to enable users to illegally modify satellite providers'
28

1 access cards, and (4) illegally facilitate the widespread distribution of NDS's
2 competitors' ROM codes and keys by publishing same on the Internet.

3 42. Plaintiffs are informed and believe that Hasak gave both the full
4 Canal+ ROM Code, as with Plaintiffs' ROM Code, to Norris with specific
5 instructions to give to Tarnovsky for the use and purpose to (1) design,
6 manufacture, and distribute to Menard signal theft devices used to circumvent the
7 technological encryption measures contained in Canal+'s access cards, as with
8 Plaintiffs' Access Cards, (2) provide software, information, and technical support
9 services relating to Canal+'s ROM Code and access cards, as with Plaintiffs' ROM
10 Code and Access Cards, and (3) facilitate the widespread distribution on the
11 Internet of the Canal+ ROM code, as with Plaintiffs' ROM Code. Tarnovsky
12 followed Hasak's and Norris's instructions of designing, manufacturing, and
13 distributing to Menard such signal theft devices, providing software, information,
14 and technical support services related to same, and posting both (1) Canal+'s ROM
15 code on www.dr7.com on March 26, 1999, and (2) Plaintiffs' ROM Code on
16 www.piratesden.com on December 24, 2000, which Tarnovsky states this is the
17 "full ECHO ROM dump" and it's "DR7's [Menard's] code."

18 43. Hasak was also aware of the real and credible threat to NDS, by its
19 competitor NagraVision, for providing DirecTV's conditional access system should
20 NDS be unable to compete due to its security system being insecure and easily
21 hacked. Plaintiffs are informed and believe that it was the perceived threat to
22 NDS's business by NagraStar that caused NDS to (1) illegally obtain and extract
23 Nagra's ROM code and keys, (2) design, manufacture, and distribute signal theft
24 devices used to circumvent the technological encryption measures contained in
25 EchoStar Access Cards for the unauthorized reception of EchoStar's DISH
26 Network satellite television programming, (3) provide software, information, and
27 technical support services relating to EchoStar Access Cards and other
28 circumvention or signal theft devices designed to enable users to illegally modify

1 EchoStar Access Cards, and (4) facilitate the widespread distribution of the Nagra
2 ROM code on the Internet. The mission of NDS's international conspiracy was
3 initiated by NDS employees Hasak, Norris, Adams, Gutman, and Segoli, among
4 others, and implemented by NDS employees and/or double agents Kommerling,
5 Tarnovsky, and Menard, among others.

6 44. Defendant Oliver Kommerling a/k/a "Alex," "ALEX," "Alexander,"
7 "Oli," "Oli K," "Oliver Kiss," and "OK" ("Kommerling") is an individual and
8 citizen of Germany, residing in Monaco. During all times relevant as stated herein,
9 Kommerling was either: (a) working for, at the direction of, and under the direct
10 and/or indirect control of NDS, and with NDS's full knowledge and/or ratification,
11 as well as for his own individual interest and/or gain, as a participant in the
12 overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a
13 wide spread compromise of Plaintiffs' conditional access system; or (b) working in
14 concert with NDS, its employees and/or agents in serving his role in the overriding
15 NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread
16 compromise of Plaintiffs' conditional access system.

17 45. Upon information and belief Defendant Oliver Kommerling is still
18 currently in possession of: (a) Plaintiffs' proprietary information including but not
19 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
20 and/or other proprietary information unlawfully extracted from the microprocessor
21 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
22 EchoStar Access Cards and/or other circumvention or signal theft devices designed
23 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
24 Security System including, but not limited to, loaders, dead processor boot boards,
25 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
26 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
27 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
28 for the unlawful and unauthorized modification of and/or access to EchoStar's

1 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
2 through the sale/distribution of, or assistance or support provided in connection
3 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
4 signal theft devices designed to enable users to illegally modify or alter EchoStar
5 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
6 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
7 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
8 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
9 other hardware and software intended for the unlawful and unauthorized
10 modification of and/or access to EchoStar's digital satellite system).

11 46. Kommerling has admitted that he worked as a consultant for NDS
12 since mid-1996. In early 1997, Kommerling helped establish NDS's Matam Centre
13 research facility in Haifa, Israel in addition to recruiting and training all NDS
14 Matam engineers.

15 47. In 1999, Kommerling and Markus Kuhn co-wrote "Design Principles
16 for Tamper Resistant Smartcards." This publication became one of the standard text
17 on how to "reverse engineer" a state-of-the-art smartcard by using certain
18 techniques including, but not limited to, acid treatments, microscopic probes, laser
19 cutting, and ion beam manipulation, among others.

20 48. Since 1996 and at all time relevant as stated herein, Kommerling
21 worked as a double agent for NDS, in a similar manner as Tarnovsky. NDS placed
22 Kommerling under deep cover in NDS's effort to maintain Kommerling's outward
23 appearance as an underground hacker/satellite pirate. In an effort to create a
24 "legitimate" outward appearance for Kommerling, a known satellite hacker and
25 pirate, NDS and Kommerling formed the company ADSR. ADSR was a
26 corporation engaged in the semi-conductor business with NDS owning 60% of the
27 shares and Kommerling owning 40% of the shares. Concerning his hacking activity
28 with NDS, Kommerling made a declaration in the *Canal+ v. NDS et al.* litigation

1 which stated, among other things, that Kommerling helped NDS obtain Canal+
2 smart cards and assisted in physically extracting the Canal+'s SECA ROM code
3 contained therein. Kommerling further declared that the code he assisted NDS in
4 extracting was the same code that was published on www.dr7.com, the website
5 owned, operated, and maintained by Menard. Specifically, Kommerling's
6 declaration accuses NDS's double agent Tarnovsky of publishing the Canal+ SECA
7 ROM code on the Internet.

8 49. During a meeting between Tarnovsky and Kommerling, Tarnovsky
9 openly admitted to Kommerling that (1) Tarnovsky received Plaintiffs' ROM Code
10 from Hasak via Norris, and (2) Tarnovsky was instructed to, and did send
11 Plaintiffs' ROM Code to Menard.

12 50. In August 1997, Kommerling contacted Marty Mullen (a/k/a Martin
13 "Marty" Paul Stewart) ("Mullen") by telephone, and introduced himself as "Ollie."
14 During this first conversation, Kommerling represented to Mullen that (1)
15 Kommerling was the first person to have a fix for DirecTV's F-card, (2)
16 Kommerling had also compromised DirecTV's H-card, and (3) Kommerling would
17 have the "DISH Network fix" very shortly. Kommerling further stated that he had
18 information that Mullen, and others acting in concert with Mullen, were planning to
19 release a software fix for DirecTV's H-card to the public. Kommerling stated that
20 if Mullen would help him out and not release the software fix for DirecTV's H-card
21 to the public just yet, Kommerling would assist Mullen in the future with DirecTV
22 software, and as a bonus, include the "DISH Network fix" once Kommerling had it
23 completed. Kommerling e-mailed his contact information to Mullen for his future
24 contact reference.

25 51. Shortly thereafter, Mullen contacted Kommerling to discuss
26 Kommerling's initial offer. During this second conversation, Kommerling stated
27 that the "DISH Network fix" was being extracted at a sophisticated laboratory in
28 Europe and that it was near completion. Kommerling also informed Mullen that

1 Kommerling was involved in establishing this new state-of-the-art laboratory that
2 could hack anything related to DISH Network. In exchange for Mullen not
3 releasing the full software fix for DirecTV's H-card, Kommerling represented that
4 he was authorized to offer Mullen an exclusive deal to distribute the software for
5 both DirecTV and DISH Network.

6 52. In February 1998, Kommerling contacted Mullen and requested that a
7 meeting be scheduled to discuss the exclusive deal for software fixes for both
8 DirecTV and DISH Network. During this third conversation, Kommerling
9 represented that the "DISH Network fix" had been completed and all relevant code
10 extracted. Kommerling further advised Mullen and that a partner of Kommerling's
11 nicknamed "Yanni" [John Luyando] would be contacting Mullen to arrange a
12 meeting.

13 53. During a meeting between Menard and Ron Ereiser, among others, on
14 or about March 8, 2001, Menard admitted to Ereiser that Kommerling also
15 approached Menard in the summer of 1998 and offered to sell Menard the full
16 Nagra ROM code for EchoStar's Access Cards for \$1,000,000. During this same
17 meeting with Kommerling, Menard admitted to Ereiser that Menard was also told
18 how the ROM dump was acquired and witnessed a demonstration of a working
19 "ECHO hack."

20 54. Defendant John Luyando a/k/a "Yanni," "Jellyfish," and "Blaster
21 ("Luyando") is an individual and citizen of the United States, residing in Norwalk,
22 Connecticut. During all times relevant as stated herein, Luyando was either: (a)
23 working for, at the direction of, and under the direct and/or indirect control of NDS,
24 and with NDS's full knowledge and/or ratification, as well as for his own individual
25 interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate
26 and/or facilitate others in effectuating a wide spread compromise of Plaintiffs'
27 conditional access system; or (b) working in concert with NDS, its employees
28 and/or agents in serving his role in the overriding NDS conspiracy to effectuate and

1 facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional
2 access system.

3 55. Upon information and belief Defendant John Luyando is still
4 currently in possession of: (a) Plaintiffs' proprietary information including but not
5 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
6 and/or other proprietary information unlawfully extracted from the microprocessor
7 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
8 EchoStar Access Cards and/or other circumvention or signal theft devices designed
9 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
10 Security System (including, but not limited to, loaders, dead processor boot boards,
11 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
12 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
13 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
14 for the unlawful and unauthorized modification of and/or access to EchoStar's
15 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
16 through the sale/distribution of, or assistance or support provided in connection
17 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
18 signal theft devices designed to enable users to illegally modify or alter EchoStar
19 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
20 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
21 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
22 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
23 other hardware and software intended for the unlawful and unauthorized
24 modification of and/or access to EchoStar's digital satellite system).

25 56. On March 13, 1998, at the direction of NDS and Kommerling,
26 Luyando met with Mullen, Archie Timuik and Joseph Lucker in Windsor, Ontario
27 to discuss Kommerling's authority to offer the "DISH Network fix," among other
28 things. During this meeting Luyando represented to Mullen that Luyando was

1 Kommerling's partner, that Luyando had Kommerling's full permission to
2 negotiate with Mullen, and that Kommerling was authorized to sell Mullen the
3 "DISH Network fix." During this meeting, at the direction of NDS and
4 Kommerling, Luyando offered Mullen the full DISH Network "ROM dump" for
5 "\$1,000,000 USD." Luyando assured Mullen that he would be the only person with
6 the fix and that he could "run with this for a long time." Luyando further
7 represented to Mullen that the DISH Network ROM dump was acquired by
8 Kommerling in a highly sophisticated laboratory. Concerning software,
9 information, and technical support services, Luyando represented that Kommerling
10 had access to "the most sophisticated equipment on the planet" and that the
11 proceeds from the sale of the "DISH Network fix" were going to be "reinvested
12 into more equipment that would help us all keep up with any new card swaps with
13 DISH Network." Luyando informed Mullen that NDS, through Kommerling,
14 instructed him to deal with Mullen first concerning a possible purchase of the
15 "DISH Network fix," but that if Mullen was not interested, to approach others with
16 the offer.

17 57. Defendant Plamen Donev a/k/a "Pluto," "Pman," "Digital," "Alien,"
18 "VIP," "Sadman," "Bolger," or "Bulgarian" ("Donev") is an individual and citizen
19 of Bulgaria, residing in Sofia, Bulgaria. During all times relevant as stated herein,
20 Donev was either: (a) working for, at the direction of, and under the direct and/or
21 indirect control of NDS, and with NDS's full knowledge and/or ratification, as
22 well as for his own individual interest and/or gain, as a participant in the overriding
23 NDS conspiracy to effectuate and/or facilitate others in effectuating a wide spread
24 compromise of Plaintiffs' conditional access system; or (b) working in concert with
25 NDS, its employees and/or agents in serving his role in the overriding NDS
26 conspiracy to effectuate and facilitate others in effectuating a wide-spread
27 compromise of Plaintiffs' conditional access system.

28

1 58. Upon information and belief Defendant Plamen Donev is still
2 currently in possession of: (a) Plaintiffs' proprietary information including but not
3 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
4 and/or other proprietary information unlawfully extracted from the microprocessor
5 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
6 EchoStar Access Cards and/or other circumvention or signal theft devices designed
7 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
8 Security System (including, but not limited to, loaders, dead processor boot boards,
9 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
10 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
11 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
12 for the unlawful and unauthorized modification of and/or access to EchoStar's
13 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
14 through the sale/distribution of, or assistance or support provided in connection
15 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
16 signal theft devices designed to enable users to illegally modify or alter EchoStar
17 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
18 loaders, dead processor boot boards, glitches, bootloaders, unloopers, emulators,
19 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
20 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
21 other hardware and software intended for the unlawful and unauthorized
22 modification of and/or access to EchoStar's digital satellite system).

23 59. Defendant Vesselin Nedeltchev a/k/a "Vesco," "VIP," "Bolger,"
24 "Vaseline," or "Bulgarian" ("Nedeltchev") is an individual and citizen of Bulgaria,
25 residing in Sofia, Bulgaria. During all times relevant as stated herein, Nedeltchev
26 was either: (a) working for, at the direction of, and under the direct and/or indirect
27 control of NDS, and with NDS's full knowledge and/or ratification, as well as for
28 his own individual interest and/or gain, as a participant in the overriding NDS

1 conspiracy to effectuate and/or facilitate others in effectuating a wide spread
2 compromise of Plaintiffs' conditional access system; or (b) working in concert with
3 NDS, its employees and/or agents in serving his role in the overriding NDS
4 conspiracy to effectuate and facilitate others in effectuating a wide-spread
5 compromise of Plaintiffs' conditional access system.

6 60. Upon information and belief Defendant Vesselin Nedeltchev is still
7 currently in possession of: (a) Plaintiffs' proprietary information including but not
8 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
9 and/or other proprietary information unlawfully extracted from the microprocessor
10 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
11 EchoStar Access Cards and/or other circumvention or signal theft devices designed
12 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
13 Security System (including, but not limited to, loaders, dead processor boot boards,
14 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
15 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
16 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
17 for the unlawful and unauthorized modification of and/or access to EchoStar's
18 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
19 through the sale/distribution of, or assistance or support provided in connection
20 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
21 signal theft devices designed to enable users to illegally modify or alter EchoStar
22 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
23 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
24 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
25 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
26 other hardware and software intended for the unlawful and unauthorized
27 modification of and/or access to EchoStar's digital satellite system).

28

1 61. Defendant Christopher Tarnovsky a/k/a “Von,” “Mike George,”
2 “MIKE,” “Mikey,” “Shrimp,” “da Shrimp,” “Code,” “Ripper,” “da Ripper Code,”
3 “Arthur von Neuman,” “Arti,” “von,” “von rat,” “Mr. Bean,” “Big Gun,” “biggun,”
4 “BG,” “Scatman,” “Tarnovsc,” “Nipper,” “Nipper Clauze,” “Nipper Clauze 00’,”
5 Nipper Clauze 2000,” “Swiss Cheeze Group,” “Swiss Cheese Productions,” “SCP,”
6 “Coleman,” “xbr21,” and “lawless1” (“Tarnovsky”) is an individual and citizen of
7 the United States, residing in California. During all times relevant as stated herein,
8 Tarnovsky was either: (a) working for, at the direction of, and under the direct
9 and/or indirect control of NDS, and with NDS’s full knowledge and/or ratification,
10 as well as for his own individual interest and/or gain, as a participant in the
11 overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a
12 wide spread compromise of Plaintiffs’ conditional access system; or (b) working in
13 concert with NDS, its employees and/or agents in serving his role in the overriding
14 NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread
15 compromise of Plaintiffs’ conditional access system.

16 62. Upon information and belief Defendant Chris Tarnovsky is still
17 currently in possession of: (a) Plaintiffs’ proprietary information including but not
18 limited to proprietary sections of Plaintiffs’ ROM code, Plaintiffs’ EEPROM code,
19 and/or other proprietary information unlawfully extracted from the microprocessor
20 embedded in Plaintiffs’ Access ‘Smart’ Cards; (b) software, hardware, Pirated
21 EchoStar Access Cards and/or other circumvention or signal theft devices designed
22 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’
23 Security System (including, but not limited to, loaders, dead processor boot boards,
24 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
25 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,
26 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
27 for the unlawful and unauthorized modification of and/or access to EchoStar’s
28 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained

1 through the sale/distribution of, or assistance or support provided in connection
2 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
3 signal theft devices designed to enable users to illegally modify or alter EchoStar
4 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
5 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
6 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
7 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
8 other hardware and software intended for the unlawful and unauthorized
9 modification of and/or access to EchoStar's digital satellite system).

10 63. Tarnovsky is a self-admitted hacker in the satellite industry and is
11 believed to have designed the first "battery cards," the first pirate technology and
12 signal theft device used to receive and satellite television programming signals
13 without authorization.

14 64. Tarnovsky has been an employee of companies linked to the News
15 Corporation, the holding company for NDS, including HarperCollins Publishers in
16 New York, although Tarnovsky never lived in New York and in reality was
17 working for NDS since as early as 1997.

18 65. Upon the instruction of NDS, Tarnovsky developed countermeasures
19 for NDS which were sold by NDS to DirecTV in order to counter-attack pirated
20 DirecTV smart cards. Tarnovsky was also an informant, or double agent, for NDS
21 and supplied NDS with information on piracy of its smart cards. On behalf of
22 NDS, and with their full knowledge, consent, instruction, and control, Tarnovsky
23 continued to receive money from Allen Menard and the West E3M group of
24 hackers and satellite pirates for his sale of software, devices, and secret codes that
25 permit programming of pirated smart cards for illegal access to the DISH Network.
26 Tarnovsky also assisted with facilitating piracy over the internet by offering patches
27 in codes and software for illegally disabling and circumventing Plaintiffs'
28 Electronic Counter Measures ("ECMs").

1 66. Tarnovsky has been employed by NDS as a double agent from as early
2 as 1997. Tarnovsky's role as NDS's double agent was to infiltrate hacking
3 organizations and to report satellite piracy information back to NDS. However,
4 upon going to work for NDS, Tarnovsky never stopped his hacking activities,
5 which NDS is fully aware of, and is one of the main reasons he was hired by NDS.
6 Upon NDS's instruction, including that by Norris, Hasak, Adams, and Gutman,
7 Tarnovsky would obtain conditional access codes for NDS's competitors from NDS
8 and then Tarnovsky would make these codes available to Menard, owner and
9 proprietor of the www.dr7.com website, for financial gain – and ultimately
10 publication. Tarnovsky was paid by NDS for his double agent work, approximately
11 \$10,000 per month, in addition to being paid by hackers for his continued hacking
12 activities, of which NDS was fully aware and openly acknowledge.

13 67. NDS, through Norris, Hasak, Adams, and Gutman, among others, were
14 all kept well informed about the double agent role of Tarnovsky and sanctioned all
15 of his hacking activities of EchoStar/NagraStar's Security System. On or about
16 October 31, 1999, Tarnovsky posted on the DR7 pirate chat forum concerning
17 EchoStar/NagraStar that "Echo is in bed with Nagra and will use same ROM for all
18 their cards around the world." On December 24, 2000, using the nickname
19 "nIpPeR cLaUz 00'," and under the direction and control of NDS, and with NDS's
20 full knowledge and ratification, Tarnovsky posted a sequence of events and data,
21 along with accompanying instructional code, that provided satellite pirates around
22 the world the 'road map' and requisite instructions for the dump of Plaintiffs' entire
23 EEPROM Code. Tarnovsky posted the foregoing, which was illegally obtained by
24 NDS in its Haifa, Israel lab and sent to Tarnovsky via Hasak and Norris with the
25 specific instructions to effectuate and assist others in effectuating a wide spread
26 compromise of Plaintiffs' conditional access system, on the Internet website
27 www.piratesden.com. In addition to allowing these satellite pirates to procure a
28 dump of Plaintiffs' EEPROM Code, the December 23 and 24, 2000 postings and

1 assistance provided by NDS, Tarnovsky and Menard, among others, also allowed
2 these same hackers to readily procure a dump of NagraStar's secret ROM Code.
3 With this assistance, satellite pirates around the world now had the all the requisite
4 proprietary information once secured in Plaintiffs' microprocessor. Specifically,
5 with this December 23 and 24, 2000 assistance by NDS, Tarnovsky and Menard,
6 among others, satellite pirates were then able to build their own card
7 reprogrammers and, thus, were able to break free from their dependence on NDS,
8 Tarnovsky and Menard, among others, for obtaining reprogrammed EchoStar
9 Access Cards. Consequently, NDS's goal of effectuating and assisting others in
10 effectuating a widespread compromise of Plaintiffs' security system began to
11 rapidly materialize.

12 68. Defendant Allen Don Juan Menard a/k/a "Al," "dr7," "Darth7,"
13 "Kelly," and "Bricklayer" d/b/a "X-Factor Design, Inc." and "NCRYPT"
14 ("Menard") is an individual and citizen of Canada, residing in Edmonton, Alberta.
15 During all times relevant as stated herein, Menard was either: (a) working for, at
16 the direction of, and under the direct and/or indirect control of NDS, and with
17 NDS's full knowledge and/or ratification, as well as for his own individual interest
18 and/or gain, as a participant in the overriding NDS conspiracy to effectuate and/or
19 facilitate others in effectuating a wide spread compromise of Plaintiffs' conditional
20 access system; or (b) working in concert with NDS, its employees and/or agents in
21 serving his role in the overriding NDS conspiracy to effectuate and facilitate others
22 in effectuating a wide-spread compromise of Plaintiffs' conditional access system.

23 69. Upon information and belief Defendant Menard is still currently in
24 possession of: (a) Plaintiffs' proprietary information including but not limited to
25 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
26 other proprietary information unlawfully extracted from the microprocessor
27 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
28 EchoStar Access Cards and/or other circumvention or signal theft devices designed

1 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
2 Security System (including, but not limited to, loaders, dead processor boot boards,
3 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
4 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
5 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
6 for the unlawful and unauthorized modification of and/or access to EchoStar's
7 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
8 through the sale/distribution of, or assistance or support provided in connection
9 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
10 signal theft devices designed to enable users to illegally modify or alter EchoStar
11 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
12 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
13 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
14 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
15 other hardware and software intended for the unlawful and unauthorized
16 modification of and/or access to EchoStar's digital satellite system).

17 70. Menard is a close personal friend, and business partner, of Tarnovsky.
18 Menard, using the fictitious name "Al" and "dr7" and doing business as "X-Factor
19 Design, Inc." and "NCRYPT," is the owner of the www.dr7.com pirate website
20 which served as a meeting and discussion place of satellite pirates world-wide.
21 Menard's website also served as Menard's business, among others, and were
22 operated and utilized as an *alter ego* of Menard, and others currently unknown to
23 Plaintiffs, for the purpose of furthering Defendants' scheme to defraud Plaintiffs.
24 Menard unlawfully published the master keys and ROM codes on www.dr7.com of
25 the following satellite providers: DirecTV, Canal+, and DISH Network. Menard
26 received these codes from NDS through Tarnovsky acting on behalf of and under
27 the control and direction of NDS.

28

1 71. Defendant Linda Wilson is an individual and citizen of Canada,
2 residing in Edmonton, Alberta. During all times relevant as stated herein, Wilson
3 was either: (a) working for, at the direction of, and under the direct and/or indirect
4 control of NDS, and with NDS's full knowledge and/or ratification, as well as for
5 her own individual interest and/or gain, as a participant in the overriding NDS
6 conspiracy to effectuate and/or facilitate others in effectuating a wide spread
7 compromise of Plaintiffs' conditional access system; or (b) working in concert with
8 NDS, its employees and/or agents in serving his role in the overriding NDS
9 conspiracy to effectuate and facilitate others in effectuating a wide-spread
10 compromise of Plaintiffs' conditional access system.

11 72. Upon information and belief Defendant Linda Wilson is still currently
12 in possession of: (a) Plaintiffs' proprietary information including but not limited to
13 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
14 other proprietary information unlawfully extracted from the microprocessor
15 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
16 EchoStar Access Cards and/or other circumvention or signal theft devices designed
17 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
18 Security System (including, but not limited to, loaders, dead processor boot boards,
19 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
20 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
21 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
22 for the unlawful and unauthorized modification of and/or access to EchoStar's
23 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
24 through the sale/distribution of, or assistance or support provided in connection
25 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
26 signal theft devices designed to enable users to illegally modify or alter EchoStar
27 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
28 loaders, dead processor boot boards, glitches, bootloaders, unloopers, emulators,

1 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
2 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
3 other hardware and software intended for the unlawful and unauthorized
4 modification of and/or access to EchoStar’s digital satellite system).

5 73. Wilson was the Registrant for the domain name of Menard’s pirate
6 website, “www.dr7.com.” Wilson is also listed as the Billing Contact and
7 Administrative Contact for Menard’s company, X-Factor Web Design, Inc., at
8 11215 Jasper Ave. NW, Suite 435, Edmonton, Alberta Canada T5K 0L5.

9 74. Defendant Mervin Main a/k/a “Rymer” (“Main”) is an individual and
10 citizen of Canada, residing in Edmonton, Alberta Canada. During all times relevant
11 as stated herein, Main was either: (a) working for, at the direction of, and under
12 the direct and/or indirect control of NDS, and with NDS’s full knowledge and/or
13 ratification, as well as for his own individual interest and/or gain, as a participant in
14 the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a
15 wide spread compromise of Plaintiffs’ conditional access system; or (b) working in
16 concert with NDS, its employees and/or agents in serving his role in the overriding
17 NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread
18 compromise of Plaintiffs’ conditional access system.

19 75. Upon information and belief Defendant Mervin Main is still currently
20 in possession of: (a) Plaintiffs’ proprietary information including but not limited to
21 proprietary sections of Plaintiffs’ ROM code, Plaintiffs’ EEPROM code, and/or
22 other proprietary information unlawfully extracted from the microprocessor
23 embedded in Plaintiffs’ Access ‘Smart’ Cards; (b) software, hardware, Pirated
24 EchoStar Access Cards and/or other circumvention or signal theft devices designed
25 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’
26 Security System (including, but not limited to, loaders, dead processor boot boards,
27 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
28 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,

1 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
2 for the unlawful and unauthorized modification of and/or access to EchoStar's
3 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
4 through the sale/distribution of, or assistance or support provided in connection
5 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
6 signal theft devices designed to enable users to illegally modify or alter EchoStar
7 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
8 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
9 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
10 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
11 other hardware and software intended for the unlawful and unauthorized
12 modification of and/or access to EchoStar's digital satellite system).

13 76. Main, using the fictitious name of "Rymer," worked for Menard and
14 his company, X-Factor Design. Main's job responsibilities included trafficking,
15 conspiring to traffic, and/or assisting others in the trafficking of: illegal drugs;
16 illegal signal theft devices; and currencies related to illegal drugs and illegal signal
17 theft devices. On or about August 30, 2001, concerning Tarnovsky's receipt of
18 \$40,100 from his mailbox address in San Marcos, Texas, a report from the Royal
19 Canadian Mounted Police's Latent Fingerprints operations matched the fingerprints
20 lifted from the "Pioneer DVD" player and the "JVC DISC" containing the currency
21 to Mervyn D. Main a/k/a "Rymer." These monies, among others, were payment
22 from Menard to Tarnovsky (via Main) for Tarnovsky's assistance in designing,
23 manufacturing, altering EchoStar Access Cards or other circumvention or signal
24 theft devices designed to enable users to illegally modify EchoStar Access Cards
25 (including, but not limited to, loaders, dead processor boot boards, glitchers,
26 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
27 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
28 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the

1 unlawful and unauthorized modification of and/or access to EchoStar's digital
2 satellite system) and providing software, information, and technical support
3 services for the continued maintenance of the illegal hack and unauthorized
4 reception of DISH Network Programming.

5 77. Defendant Dave Dawson a/k/a "JD," "Dave," or "Jack Daniels" d/b/a
6 "Discount Satellite," "DiscSat," or "DSSCanada" ("Dawson") is an individual and
7 citizen of Canada, residing in Edmonton, Alberta. During all times relevant as
8 stated herein, Dawson was either: (a) working for, at the direction of, and under
9 the direct and/or indirect control of NDS, and with NDS's full knowledge and/or
10 ratification, as well as for his own individual interest and/or gain, as a participant in
11 the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a
12 wide spread compromise of Plaintiffs' conditional access system; or (b) working in
13 concert with NDS, its employees and/or agents in serving his role in the overriding
14 NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread
15 compromise of Plaintiffs' conditional access system.

16 78. Upon information and belief Defendant Dave Dawson is still currently
17 in possession of: (a) Plaintiffs' proprietary information including but not limited to
18 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
19 other proprietary information unlawfully extracted from the microprocessor
20 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
21 EchoStar Access Cards and/or other circumvention or signal theft devices designed
22 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
23 Security System (including, but not limited to, loaders, dead processor boot boards,
24 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
25 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
26 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
27 for the unlawful and unauthorized modification of and/or access to EchoStar's
28 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained

1 through the sale/distribution of, or assistance or support provided in connection
2 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
3 signal theft devices designed to enable users to illegally modify or alter EchoStar
4 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
5 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
6 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
7 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
8 other hardware and software intended for the unlawful and unauthorized
9 modification of and/or access to EchoStar's digital satellite system).

10 79. Dawson, using the fictitious names of "JD," "Jack Daniels," and
11 "Dave" and doing business as "Discount Satellite," "DiscSat," and "DSScanada,"
12 was one of the pirate dealers working under Menard who was involved with selling
13 Pirated EchoStar Access Cards and other circumvention or signal theft devices
14 designed to enable users to illegally modify EchoStar Access Cards (including, but
15 not limited to, loaders, dead processor boot boards, glitchers, bootloaders,
16 unloopers, emulators, printed circuit boards, programmers, integrated
17 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
18 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
19 unlawful and unauthorized modification of and/or access to EchoStar's digital
20 satellite system). Dawson received his Pirated EchoStar Access Cards from Menard
21 and, in turn, acted as a "dealer" and distributed and sold Pirated EchoStar Access
22 Cards and other circumvention or signal theft devices designed to enable users to
23 illegally modify EchoStar Access Cards (including, but not limited to, loaders, dead
24 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
25 boards, programmers, integrated receivers/decoders, Audio Video Replicators
26 "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
27 and software intended for the unlawful and unauthorized modification of and/or
28 access to EchoStar's digital satellite system) for profit. Dawson also advertised the

1 sale of Pirated EchoStar Access Cards and other circumvention or signal theft
2 devices designed to enable users to illegally modify EchoStar Access Cards
3 (including, but not limited to, loaders, dead processor boot boards, glitchers,
4 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
5 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
6 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
7 unlawful and unauthorized modification of and/or access to EchoStar’s digital
8 satellite system) in the State of California and elsewhere through advertisements
9 placed by Dawson in one or more “underground” satellite pirate publications, and
10 through his Internet websites, www.discountsatellite.com and
11 www.DSScanada.com, and email addresses created, operated, and maintained by
12 Dawson. Upon information and belief, Discount Satellite, DiscSat, and DSScanada
13 are or were operated and utilized as an *alter ego* of Dawson, and others currently
14 unknown to Plaintiffs, for the purpose of furthering Defendants’ scheme to defraud
15 Plaintiffs. Dawson engaged in the sale of Pirated EchoStar Access Cards and other
16 circumvention or signal theft devices designed to enable users to illegally modify
17 EchoStar Access Cards (including, but not limited to, loaders, dead processor boot
18 boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards,
19 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”
20 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
21 software intended for the unlawful and unauthorized modification of and/or access
22 to EchoStar’s digital satellite system) in the United States.

23 80. Defendant Shawn Quinn a/k/a “Hitec” d/b/a “HitecSatellite” and
24 “HitecSat” (“Quinn”) is an individual and citizen of Canada, residing in British
25 Columbia. During all times relevant as stated herein, Quinn was either: (a)
26 working for, at the direction of, and under the direct and/or indirect control of NDS,
27 and with NDS’s full knowledge and/or ratification, as well as for his own individual
28 interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate

1 and/or facilitate others in effectuating a wide spread compromise of Plaintiffs'
2 conditional access system; or (b) working in concert with NDS, its employees
3 and/or agents in serving his role in the overriding NDS conspiracy to effectuate and
4 facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional
5 access system.

6 81. Upon information and belief Defendant Quinn is still currently in
7 possession of: (a) Plaintiffs' proprietary information including but not limited to
8 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
9 other proprietary information unlawfully extracted from the microprocessor
10 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
11 EchoStar Access Cards and/or other circumvention or signal theft devices designed
12 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
13 Security System (including, but not limited to, loaders, dead processor boot boards,
14 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
15 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
16 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
17 for the unlawful and unauthorized modification of and/or access to EchoStar's
18 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
19 through the sale/distribution of, or assistance or support provided in connection
20 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
21 signal theft devices designed to enable users to illegally modify or alter EchoStar
22 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
23 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
24 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
25 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
26 other hardware and software intended for the unlawful and unauthorized
27 modification of and/or access to EchoStar's digital satellite system).

28

1 82. Quinn, using the fictitious name “Hitec” and doing business as
2 “HitecSatellite” and “HitecSat,” was one of the pirate dealers working under
3 Menard who was selling Pirated EchoStar Access Cards and other circumvention or
4 signal theft devices designed to enable users to illegally modify EchoStar Access
5 Cards (including, but not limited to, loaders, dead processor boot boards, glitchers,
6 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
7 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
8 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
9 unlawful and unauthorized modification of and/or access to EchoStar’s digital
10 satellite system). Quinn received his Pirated EchoStar Access Cards from Menard
11 and, in turn, acted as a “dealer” and distributed and sold the Pirated EchoStar
12 Access Cards and other circumvention or signal theft devices designed to enable
13 users to illegally modify EchoStar Access Cards (including, but not limited to,
14 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
15 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
16 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
17 other hardware and software intended for the unlawful and unauthorized
18 modification of and/or access to EchoStar’s digital satellite system) for profit.
19 Quinn also advertised the sale of Pirated EchoStar Access Cards and other
20 circumvention or signal theft devices designed to enable users to illegally modify
21 EchoStar Access Cards (including, but not limited to, loaders, dead processor boot
22 boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards,
23 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”
24 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
25 software intended for the unlawful and unauthorized modification of and/or access
26 to EchoStar’s digital satellite system) in the State of California and elsewhere
27 through advertisements placed by Quinn in one or more “underground” satellite
28 pirate publications, and through his Internet website, www.hitecsat.com, and email

1 addresses created, operated, and maintained by Quinn. Upon information and
2 belief, "HitecSatellite" and "HitecSat" are or have been operated and utilized as an
3 *alter ego* of Quinn and others currently unknown to Plaintiffs for the purpose of
4 furthering Defendants' scheme to defraud Plaintiffs. Quinn engaged in the sale of
5 Pirated EchoStar Access Cards and other circumvention or signal theft devices
6 designed to enable users to illegally modify EchoStar Access Cards (including, but
7 not limited to, loaders, dead processor boot boards, glitches, bootloaders,
8 unloopers, emulators, printed circuit boards, programmers, integrated
9 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
10 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
11 unlawful and unauthorized modification of and/or access to EchoStar's digital
12 satellite system) in the United States.

13 83. Defendant Andre Sergei a/k/a "Koin" d/b/a "Koinvizion" ("Sergei") is
14 an individual and citizen of Canada, residing in British Columbia. During all times
15 relevant as stated herein, Sergei was either: (a) working for, at the direction of, and
16 under the direct and/or indirect control of NDS, and with NDS's full knowledge
17 and/or ratification, as well as for his own individual interest and/or gain, as a
18 participant in the overriding NDS conspiracy to effectuate and/or facilitate others in
19 effectuating a wide spread compromise of Plaintiffs' conditional access system; or
20 (b) working in concert with NDS, its employees and/or agents in serving his role in
21 the overriding NDS conspiracy to effectuate and facilitate others in effectuating a
22 wide-spread compromise of Plaintiffs' conditional access system.

23 84. Upon information and belief Defendant Andre Sergei is still currently
24 in possession of: (a) Plaintiffs' proprietary information including but not limited to
25 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
26 other proprietary information unlawfully extracted from the microprocessor
27 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
28 EchoStar Access Cards and/or other circumvention or signal theft devices designed

1 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’
2 Security System (including, but not limited to, loaders, dead processor boot boards,
3 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
4 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,
5 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
6 for the unlawful and unauthorized modification of and/or access to EchoStar’s
7 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
8 through the sale/distribution of, or assistance or support provided in connection
9 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
10 signal theft devices designed to enable users to illegally modify or alter EchoStar
11 Access Cards and/or Plaintiffs’ Security System (including, but not limited to,
12 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
13 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
14 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
15 other hardware and software intended for the unlawful and unauthorized
16 modification of and/or access to EchoStar’s digital satellite system).

17 85. Sergei, using the fictitious name “Koin” and doing business as
18 “Koinvizion,” was one of the pirate dealers working under Menard who was selling
19 Pirated EchoStar Access Cards and other circumvention or signal theft devices
20 designed to enable users to illegally modify EchoStar Access Cards (including, but
21 not limited to, loaders, dead processor boot boards, glitchers, bootloaders,
22 unloopers, emulators, printed circuit boards, programmers, integrated
23 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
24 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
25 unlawful and unauthorized modification of and/or access to EchoStar’s digital
26 satellite system). Sergei received his Pirated EchoStar Access Cards from Menard
27 and, in turn, acted as a “dealer” and distributed and sold the Pirated EchoStar
28 Access Cards and other circumvention or signal theft devices designed to enable

1 users to illegally modify EchoStar Access Cards (including, but not limited to,
2 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
3 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
4 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
5 other hardware and software intended for the unlawful and unauthorized
6 modification of and/or access to EchoStar’s digital satellite system) for profit.
7 Sergei also advertised the sale of Pirated EchoStar Access Cards and other
8 circumvention or signal theft devices designed to enable users to illegally modify
9 EchoStar Access Cards (including, but not limited to, loaders, dead processor boot
10 boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards,
11 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”
12 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
13 software intended for the unlawful and unauthorized modification of and/or access
14 to EchoStar’s digital satellite system) in the State of California and elsewhere
15 through advertisements placed by Sergei in one or more “underground” satellite
16 pirate publications, and through his internet website, www.koinvizion.com, and
17 email addresses created, operated, and maintained by Sergei. Upon information
18 and belief, Koinvizion is or has been operated and utilized as an *alter ego* of Sergei
19 and others currently unknown to Plaintiffs for the purpose of furthering Defendants’
20 scheme to defraud Plaintiffs. Sergei engaged in the sale of Pirated EchoStar Access
21 Cards and other circumvention or signal theft devices designed to enable users to
22 illegally modify EchoStar Access Cards (including, but not limited to, loaders, dead
23 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
24 boards, programmers, integrated receivers/decoders, Audio Video Replicators
25 “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
26 and software intended for the unlawful and unauthorized modification of and/or
27 access to EchoStar’s digital satellite system) in the United States.

28

1 86. Defendant Stanley Frost a/k/a “Frosty,” “wheels,” “wheels,” d/b/a
2 “The New Frontier Group,” f/k/a “The Blazer Group” (“Frost”) is an individual and
3 citizen of the United State, residing in New York, New York. During all times
4 relevant as stated herein, Frost was either: (a) working for, at the direction of, and
5 under the direct and/or indirect control of NDS, and with NDS’s full knowledge
6 and/or ratification, as well as for his own individual interest and/or gain, as a
7 participant in the overriding NDS conspiracy to effectuate and/or facilitate others in
8 effectuating a wide spread compromise of Plaintiffs’ conditional access system; or
9 (b) working in concert with NDS, its employees and/or agents in serving his role in
10 the overriding NDS conspiracy to effectuate and facilitate others in effectuating a
11 wide-spread compromise of Plaintiffs’ conditional access system.

12 87. Upon information and belief Defendant Stan Frost is still currently in
13 possession of: (a) Plaintiffs’ proprietary information including but not limited to
14 proprietary sections of Plaintiffs’ ROM code, Plaintiffs’ EEPROM code, and/or
15 other proprietary information unlawfully extracted from the microprocessor
16 embedded in Plaintiffs’ Access ‘Smart’ Cards; (b) software, hardware, Pirated
17 EchoStar Access Cards and/or other circumvention or signal theft devices designed
18 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’
19 Security System (including, but not limited to, loaders, dead processor boot boards,
20 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
21 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,
22 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
23 for the unlawful and unauthorized modification of and/or access to EchoStar’s
24 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
25 through the sale/distribution of, or assistance or support provided in connection
26 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
27 signal theft devices designed to enable users to illegally modify or alter EchoStar
28 Access Cards and/or Plaintiffs’ Security System (including, but not limited to,

1 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
2 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
3 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
4 other hardware and software intended for the unlawful and unauthorized
5 modification of and/or access to EchoStar’s digital satellite system).

6 88. Frost, using the fictitious name “Frosty” and doing business as “The
7 New Frontier Group,” was one of the pirate dealers working under Menard who
8 was selling Pirated EchoStar Access Cards and other circumvention or signal theft
9 devices designed to enable users to illegally modify EchoStar Access Cards
10 (including, but not limited to, loaders, dead processor boot boards, glitchers,
11 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
12 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
13 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
14 unlawful and unauthorized modification of and/or access to EchoStar’s digital
15 satellite system). Frost received his Pirated EchoStar Access Cards from Menard
16 and, in turn, acted as a “dealer” and distributed and sold the Pirated EchoStar
17 Access Cards and other circumvention or signal theft devices designed to enable
18 users to illegally modify EchoStar Access Cards (including, but not limited to,
19 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
20 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
21 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
22 other hardware and software intended for the unlawful and unauthorized
23 modification of and/or access to EchoStar’s digital satellite system) for profit.
24 Frost also advertised the sale of Pirated EchoStar Access Cards and other
25 circumvention or signal theft devices designed to enable users to illegally modify
26 EchoStar Access Cards (including, but not limited to, loaders, dead processor boot
27 boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards,
28 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”

1 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
2 software intended for the unlawful and unauthorized modification of and/or access
3 to EchoStar's digital satellite system) in the State of California and elsewhere
4 through advertisements placed by Frost in one or more "underground" satellite
5 pirate publications, and through his Internet website, www.newfrontiergroup.com,
6 and email addresses created, operated, and maintained by Dawson. Upon
7 information and belief, The New Frontier Group is or was operated and utilized as
8 an *alter ego* of Frost, and others currently unknown to Plaintiffs, for the purpose of
9 furthering Defendants' scheme to defraud Plaintiffs. Frost engaged in the sale of
10 Pirated EchoStar Access Cards and other circumvention or signal theft devices
11 designed to enable users to illegally modify EchoStar Access Cards (including, but
12 not limited to, loaders, dead processor boot boards, glitches, bootloaders,
13 unloopers, emulators, printed circuit boards, programmers, integrated
14 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
15 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
16 unlawful and unauthorized modification of and/or access to EchoStar's digital
17 satellite system) in the United States.

18 89. Defendant Todd Dale ("Dale") is an individual and citizen of Canada,
19 residing in Edmonton, Alberta. During all times relevant as stated herein, Dale was
20 either: (a) working for, at the direction of, and under the direct and/or indirect
21 control of NDS, and with NDS's full knowledge and/or ratification, as well as for
22 his own individual interest and/or gain, as a participant in the overriding NDS
23 conspiracy to effectuate and/or facilitate others in effectuating a wide spread
24 compromise of Plaintiffs' conditional access system; or (b) working in concert with
25 NDS, its employees and/or agents in serving his role in the overriding NDS
26 conspiracy to effectuate and facilitate others in effectuating a wide-spread
27 compromise of Plaintiffs' conditional access system.

28

1 90. Upon information and belief Defendant Todd Dale is still currently in
2 possession of: (a) Plaintiffs' proprietary information including but not limited to
3 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or
4 other proprietary information unlawfully extracted from the microprocessor
5 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
6 EchoStar Access Cards and/or other circumvention or signal theft devices designed
7 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
8 Security System (including, but not limited to, loaders, dead processor boot boards,
9 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
10 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
11 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
12 for the unlawful and unauthorized modification of and/or access to EchoStar's
13 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
14 through the sale/distribution of, or assistance or support provided in connection
15 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
16 signal theft devices designed to enable users to illegally modify or alter EchoStar
17 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
18 loaders, dead processor boot boards, glitches, bootloaders, unloopers, emulators,
19 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
20 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
21 other hardware and software intended for the unlawful and unauthorized
22 modification of and/or access to EchoStar's digital satellite system).

23 91. Dale was one of the pirate dealers working under Menard who was
24 selling Pirated EchoStar Access Cards and other circumvention or signal theft
25 devices designed to enable users to illegally modify EchoStar Access Cards
26 (including, but not limited to, loaders, dead processor boot boards, glitches,
27 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
28 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA

1 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
2 unlawful and unauthorized modification of and/or access to EchoStar’s digital
3 satellite system). Dale received his Pirated EchoStar Access Cards from Menard
4 and, in turn, acted as a “dealer” and distributed and sold the Pirated EchoStar
5 Access Cards and other circumvention or signal theft devices designed to enable
6 users to illegally modify EchoStar Access Cards (including, but not limited to,
7 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
8 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
9 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
10 other hardware and software intended for the unlawful and unauthorized
11 modification of and/or access to EchoStar’s digital satellite system) for profit. Dale
12 engaged in the sale of Pirated EchoStar Access Cards and other circumvention or
13 signal theft devices designed to enable users to illegally modify EchoStar Access
14 Cards (including, but not limited to, loaders, dead processor boot boards, glitchers,
15 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
16 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
17 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
18 unlawful and unauthorized modification of and/or access to EchoStar’s digital
19 satellite system) in the United States.

20 92. Defendant George Tarnovsky (“Tarnovsky Sr.”) is an individual and
21 citizen of the United States, residing in Virginia. During all times relevant as stated
22 herein, Tarnovsky Sr. was either: (a) working for, at the direction of, and under the
23 direct and/or indirect control of NDS, and with NDS’s full knowledge and/or
24 ratification, as well as for his own individual interest and/or gain, as a participant in
25 the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a
26 wide spread compromise of Plaintiffs’ conditional access system; or (b) working in
27 concert with NDS, its employees and/or agents in serving his role in the overriding
28

1 NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread
2 compromise of Plaintiffs' conditional access system.

3 93. Upon information and belief Defendant George Tarnovsky is still
4 currently in possession of: (a) Plaintiffs' proprietary information including but not
5 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
6 and/or other proprietary information unlawfully extracted from the microprocessor
7 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
8 EchoStar Access Cards and/or other circumvention or signal theft devices designed
9 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
10 Security System (including, but not limited to, loaders, dead processor boot boards,
11 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
12 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
13 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
14 for the unlawful and unauthorized modification of and/or access to EchoStar's
15 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
16 through the sale/distribution of, or assistance or support provided in connection
17 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
18 signal theft devices designed to enable users to illegally modify or alter EchoStar
19 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
20 loaders, dead processor boot boards, glitches, bootloaders, unloopers, emulators,
21 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
22 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
23 other hardware and software intended for the unlawful and unauthorized
24 modification of and/or access to EchoStar's digital satellite system).

25 94. Defendant Brian Sommerfield a/k/a "HeeD" ("Sommerfield") is an
26 individual and citizen of Canada, residing in British Columbia. During all times
27 relevant as stated herein, Sommerfield was either: (a) working for, at the direction
28 of, and under the direct and/or indirect control of NDS, and with NDS's full

1 knowledge and/or ratification, as well as for his own individual interest and/or gain,
2 as a participant in the overriding NDS conspiracy to effectuate and/or facilitate
3 others in effectuating a wide spread compromise of Plaintiffs' conditional access
4 system; or (b) working in concert with NDS, its employees and/or agents in serving
5 his role in the overriding NDS conspiracy to effectuate and facilitate others in
6 effectuating a wide-spread compromise of Plaintiffs' conditional access system.

7 95. Upon information and belief Defendant Brian Sommerfield is still
8 currently in possession of: (a) Plaintiffs' proprietary information including but not
9 limited to proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code,
10 and/or other proprietary information unlawfully extracted from the microprocessor
11 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
12 EchoStar Access Cards and/or other circumvention or signal theft devices designed
13 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
14 Security System (including, but not limited to, loaders, dead processor boot boards,
15 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
16 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
17 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
18 for the unlawful and unauthorized modification of and/or access to EchoStar's
19 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
20 through the sale/distribution of, or assistance or support provided in connection
21 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
22 signal theft devices designed to enable users to illegally modify or alter EchoStar
23 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
24 loaders, dead processor boot boards, glitches, bootloaders, unloopers, emulators,
25 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
26 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
27 other hardware and software intended for the unlawful and unauthorized
28 modification of and/or access to EchoStar's digital satellite system).

1 96. Defendant Ed Bruce a/k/a “Stoxxx” (“Bruce”) is an individual and
2 citizen of Canada, residing in British Columbia. During all times relevant as stated
3 herein, Bruce was either: (a) working for, at the direction of, and under the direct
4 and/or indirect control of NDS, and with NDS’s full knowledge and/or ratification,
5 as well as for his own individual interest and/or gain, as a participant in the
6 overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a
7 wide spread compromise of Plaintiffs’ conditional access system; or (b) working in
8 concert with NDS, its employees and/or agents in serving his role in the overriding
9 NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread
10 compromise of Plaintiffs’ conditional access system.

11 97. Upon information and belief Defendant Ed Bruce is still currently in
12 possession of: (a) Plaintiffs’ proprietary information including but not limited to
13 proprietary sections of Plaintiffs’ ROM code, Plaintiffs’ EEPROM code, and/or
14 other proprietary information unlawfully extracted from the microprocessor
15 embedded in Plaintiffs’ Access ‘Smart’ Cards; (b) software, hardware, Pirated
16 EchoStar Access Cards and/or other circumvention or signal theft devices designed
17 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’
18 Security System (including, but not limited to, loaders, dead processor boot boards,
19 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
20 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,
21 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
22 for the unlawful and unauthorized modification of and/or access to EchoStar’s
23 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
24 through the sale/distribution of, or assistance or support provided in connection
25 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
26 signal theft devices designed to enable users to illegally modify or alter EchoStar
27 Access Cards and/or Plaintiffs’ Security System (including, but not limited to,
28 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,

1 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
2 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
3 other hardware and software intended for the unlawful and unauthorized
4 modification of and/or access to EchoStar’s digital satellite system).

5 98. Defendant “Beavis” true identity unknown at this time.

6 99. Defendant “jazzercz” true identity unknown at this time.

7 100. Defendant “Stuntguy” true identity unknown at this time.

8 101. Defendants John Does 1 through 100 are individuals and entities
9 whose names are currently unknown to Plaintiffs and who have acted in concert
10 with Defendants and participated in the acts and practices alleged herein. Upon
11 information and belief, John Does 1 through 100 includes individuals and entities
12 currently located in the United States and Canada, among other locations.

13 102. Unless indicated otherwise, the term “Defendants,” as used herein,
14 refers to “Defendants and/or their employees, agents, or persons and/or entities
15 acting at the direction and under the direct or indirect control of Defendants, and
16 with their full knowledge and/or ratification, and/or those persons and/or entities
17 acting in concert with Defendants and/or their employees and/or agents, as well as
18 for their own individual interest, pursuant to and in furtherance of the overriding
19 NDS conspiracy, as alleged herein, by cooperating with, aiding and abetting, and/or
20 ratifying and adopting each of the acts of the remaining Defendants and/or other
21 members of the conspiracy by engaging in the acts alleged herein.”

22 **IV. PLAINTIFFS’ & DEFENDANT NDS’S SECURITY SYSTEMS**

23 **A. The Components of Plaintiffs’ Security System**

24 103. A consumer wishing to subscribe to EchoStar Programming on the
25 DISH Network must first have the necessary equipment, which consists primarily
26 of: (1) a satellite dish antenna (“dish”); (2) an integrated receiver/decoder (“IRD”,
27 “receiver” or “set-top box”); and (3) a credit card-sized EchoStar Access Card
28 (“Smart Card” or “Access Card”).

1 104. EchoStar Smart Cards are purchased from NagraStar and are provided
2 by EchoStar to the subscriber for use in connection with the set-top box for the sole
3 purpose of enabling legally authorized access to the DISH Network. Subscribers
4 are not authorized to modify Smart Cards. Smart Cards are clearly marked as the
5 property of EchoStar and must be returned upon request. EchoStar's ownership of
6 its Smart Cards is explained in the subscriber's agreement with EchoStar:

7
8 The Smart Card remains the property of EchoStar . . . and
9 any tampering or unauthorized modification to the Smart
10 Card is strictly prohibited and may result in, and subject
11 you to, legal action. You agree to return the Smart Card
12 to us upon request. EchoStar therefore retains the right to
demand return of the Access Card at any time. EchoStar
does not authorize anyone to modify the Access Card or
the microprocessor housed on the Access Card, in any
manner.

13 105. EchoStar Smart Cards are essential to the operation of the DISH
14 Network service, in part, because they contain a microprocessor chip that stores
15 data and encryption technology, communicates with the set-top-box enabling the
16 decryption of the satellite signal transmitted from EchoStar, and performs various
17 computing and customer entitlement functions. Plaintiffs' Smart Card is, in and of
18 itself, a secure computer which contains, among other things, a microprocessor unit.
19 The microprocessor unit performs routine calculations that enables, among other
20 things, the Smart Card and set-top box (IRD) to communicate with one another
21 resulting in the unscrambling of EchoStar's satellite signal enabling authorized
22 subscribers access to EchoStar Programming.

23 106. The microprocessor unit is supported in part by two segments of
24 memory: (1) Read-Only-Memory ("ROM"); and (2) Electronically Erasable
25 Programmable Read-Only-Memory ("EEPROM"). Generally, the ROM Code
26 segment contains code from which intimate knowledge and information about
27 Plaintiffs' Security System and how it works can be derived; whereas, the
28 EEPROM Code segment contains secret keys enabling the decryption of EchoStar's

1 satellite signal. In order for a pirate to fully develop a “hack” for Plaintiffs’ Security
2 System, the pirate must have the detailed information and intimate knowledge of
3 the code memcry contained in both the ROM Code segment and the EEPROM
4 Code segment of Plaintiffs’ Smart Card.

5 107. The ROM Code segment provides detailed instructions and commands
6 to Plaintiffs’ Smart Cards and set-top boxes in the normal operation of Plaintiffs’
7 Security System. The “Nagra ROM Code” is the quintessential component of
8 Plaintiffs’ Security System and access to the detailed information and intimate
9 knowledge contained therein is mandatory for a pirate trying to unlock the safe to
10 Plaintiffs’ secrets controlling Plaintiffs’ Security System.

11 108. The EEPROM Code segment stores data and can potentially store code
12 commands that have been written to the Smart Card which remains even if the
13 Smart Card does not have power, but which can be erased and modified. The
14 EEPROM Code contains data that the ROM Code segment reads from in
15 performing its calculation and operation functions. The EEPROM Code segment
16 contains secret “transmission” keys (Sometimes called "decrypt keys NN" in illegal
17 internet posts), and secret “pairing” keys (Sometimes called "Secret boxkey” in
18 illegal internet posts). The “pairing keys” are used to encrypt and decrypt the
19 communications between the Smart Card and the set-top box (IRD).

20 109. EchoStar frequently communicates with the microprocessor chip on
21 the Smart Card by sending and receiving information which is routinely updated.
22 The information transmitted to and temporarily stored on the Smart Card
23 microprocessor and in related memory, includes the most recent software code
24 related to the functioning of certain portions of the Security System.

25 110. At the first activation of a customer’s set-top box, EchoStar sends a
26 signal to the Smart Card in order to “pair” the Smart Card to the set-top box. Both
27 the Smart Card and set-top box have a unique identification number that is
28 maintained by EchoStar’s subscriber management system. This pairing operation,

1 utilizing the two unique identification numbers, is mandatory for the proper
2 operation of the Security System.

3 111. Plaintiffs' Security System effectively controls access to copyrighted
4 works included in DISH Network programming. In addition, the Security System
5 ensures that the protection afforded to this copyrighted material, such as limitations
6 on the dissemination and use in accordance with EchoStar's contractual agreements
7 with content providers, is preserved.

8
9 **A. NDS was Fully Compromised as Early as 1995 and Was Losing
10 Credibility in the Conditional Access System Market Place**

11 112. Three companies manufacture the majority of "conditional access
12 systems" for the Direct-to-Home Broadcast Satellite ("DBS") industry worldwide.
13 Two of those companies are NDS and its related companies, and NagraStar and its
14 related companies, including the Kudelski Group.

15 113. NDS supplies the conditional access system used by, among others,
16 DirecTV, a DBS company in the United States and competitor of EchoStar.

17 114. In 1995, a group of hackers successfully defeated the NDS Security
18 System employed by DirecTV. The results of the hackers' work were published on
19 the Internet which led to the design, manufacture, and sale of certain circumvention
20 or signal theft devices that were used by hackers and signal "pirates" to unlawfully
21 intercept and view DirecTV-brand satellite television programming.

22 115. After its Security System had been fully compromised and NDS
23 became aware of its inferior technology and its inability to maintain the integrity of
24 its Security System, NDS made a conscious decision to hire and "control" all of the
25 most well-known, or "best" satellite pirates and hackers. NDS was able to dictate
26 when its Smart Cards would be hacked, and thus, could continue to make money
27
28

1 from its customers, such as DirecTV, for Smart Card swap-outs and for providing
2 electronic countermeasures to the NDS hackers' latest piracy efforts.

3 116. NDS made the conscious decision to manipulate the hacking of its own
4 Security System and to get the most possible financial gain from the hack of its
5 Smart Card. With most of the world's best pirates on its payroll, on or about
6 February 1997, NDS superficially attempted to "remedy" certain problems plaguing
7 their Security System by releasing a second-generation smart card, known in the
8 industry as the "P2" card.

9 117. NDS convinced DirecTV to initiate a "swap out" program, whereby all
10 first generation cards, the NDS "P1" cards, were exchanged for NDS "P2" cards at
11 DirecTV's expense – costing millions of dollars. During this swap out period,
12 DirecTV used both the "P1" and "P2" conditional access systems. On or about July
13 7, 1997, the swap out was complete and the "P1" system was shut down
14 completely.

15 118. Unfortunately for DirecTV, because NDS had put all of the world's
16 best hackers on its payroll, NDS was fully aware of, and sanctioned, the hack of its
17 P2 cards, notwithstanding the swap out agreed to by DirecTV. By the end of
18 August 1997 the new "P2" system had been successfully hacked, leaving DirecTV
19 with nothing to show for its expensive Smart Card swap out. Once again, DirecTV
20 was left with a compromised NDS conditional access system.

21 119. Although the NDS systems had been compromised multiple times, in
22 the summer of 1998, it was still believed that Plaintiffs' Security System had not
23 been defeated by pirates or hackers.

24 120. Plaintiffs believe that one reason why its Security System had not been
25 defeated by hackers is because the level of technology needed to accomplish such
26 an invasive attack on EchoStar's Access Card could only be found in a handful of
27 laboratories in the world which are not accessible to hackers or pirates. NDS owns
28 one such laboratory in Haifa, Israel.

1 **C. At DirecTV's Request, in 1998 the Kudelski Group Competed**
2 **With NDS for a Bid to Replace NDS's Security System With**
3 **Nagravision as the Security System to be Used by DirecTV**

4 121. In the summer of 1998, DirecTV put out a Request for Information
5 because they were considering replacing NDS as their Security System provider,
6 due to the problems DirecTV was having with the piracy and hacking of NDS's
7 inferior Smart Card technology.

8 122. After submitting a proposal to DirecTV in the fall of 1998, the
9 Kudelski Group was the only company invited to respond to a formal Request for
10 Proposal. Upon information and belief, DirecTV did not engage in discussions
11 with NDS regarding the extension or renewal of its contract, instead electing to
12 negotiate exclusively with the Kudelski Group.

13 123. In fact, DirecTV specifically requested that the Kudelski Group
14 develop a plan for the conversion of the NagraStar Security System from the NDS
15 system to one that is based upon the NagraStar technology, and to set forth the
16 details of the Kudelski Group's plan in a "White Paper."

17
18 **V. PLAINTIFFS' MOTION TO INTERVENE IN THE CANAL+ V. NDS**
19 **LITIGATION**

20 **A. On September 27, 2002, Plaintiffs Filed a Motion to Intervene in**
21 **the Canal + v. NDS Litigation, Which Concerned Allegations that**
22 **NDS Had Cracked Canal+'s Security System Using the Same**
23 **Common Plan NDS Employed to Attack Plaintiffs' Security**
24 **System**

25 124. Hacking Plaintiffs' Security System is not the first time NDS has
26 engaged in wrongful behavior against a competitor's Security System. On or about
27 April 9, 2002, Oliver Kommerling, NDS's employee and agent, explained the
28

1 methods that NDS used to break the Security System of another encryption
2 competitor, Canal+, and to distribute that information to foster satellite piracy.

3 125. Kommerling testified that “NDS engineers in the NDS facility in
4 Haifa, Israel obtained Canal+ smart cards and using the techniques taught by me
5 [Kommerling] (some of which were described in my paper Design Principles for
6 Tamper Resistant Smartcards written with Markus Kuhn) were able to physically
7 extract the Canal+ machine code embedded in their smart cards.” Further
8 Kommerling testified that “NDS engineers disassembled and analyzed the extracted
9 machine code . . .” which was later confirmed by Kommerling as the same code
10 that was published on the “DR7 website” by NDS agent Christopher Tarnovsky.
11 (Kommerling Dec. ¶ 6(a)-(e), attached hereto.)

12 126. Upon further investigation, EchoStar discovered the sworn declaration
13 of Jan Saggiori, an employee of SSS LLC, based in Geneva Switzerland. Saggiori
14 testified that he “asked Chris Tarnovsky if he could obtain the [missing] code
15 present at the 2000 address from Al Menart. By an email exchange from Chris
16 Tarnovsky, Chris sent me [Saggiori] an 8kb binary file that he claimed contained
17 the requested code extracted from the Canal+ smart card.” (Saggiori Dec. ¶ 5 and
18 Exhibits to his declaration, attached hereto)

19 127. Upon Plaintiffs’ receipt and review of the code sent from NDS
20 employee Tarnovsky on or about March 28, 1999, it was discovered that the code
21 sent was actually from an ST microchip that NagraStar used within its Smart Cards.
22 As evidenced by this code, and the well pleaded facts herein, Plaintiffs are now
23 informed and believe that NDS may have cracked Plaintiffs’ Security System as
24 early as March 28, 1999, and distributed Plaintiffs’ illegally obtained code at thist
25 time through its employee and agent, Christopher Tarnovsky and other Defendants,
26 with the intent and common plan to facilitate the piracy of Plaintiffs’ Security
27 System and cause harm to Plaintiffs.
28

1 128. Plaintiffs discovered for the first time that NDS was responsible for the
2 acts complained of herein in approximately early September 2002 and immediately
3 brought an action against NDS on September 27, 2002, by filing a Motion to
4 Intervene in Canal+'s pending lawsuit against NDS – which was based upon similar
5 facts and circumstances. The *Canal + v. NDS et al.* case settled before Plaintiffs'
6 Motion to Intervene was heard. Accordingly, Plaintiffs immediately filed this suit
7 on June 6, 2003.

8
9 **VI. DEFENDANTS' CONSPIRACY, COMMON PLAN & UNLAWFUL**
10 **CONDUCT**

11 **A. PHASE 1: NDS Hires the World's most Infamous Hackers in**
12 **order to "Control" the Hacking of its Smart Cards and Security**
13 **System -- in Lieu of Improving its Technology.**

14 129. On or about September 26, 1997, an NDS Memorandum Report to
15 Hasak, entitled the "Main Story" which illuminates the grave status concerning the
16 reputation and commercial well being of NDS, states in relevant part:

17 **MAIN STORY**

18 *At present I think we are on the edge of a serious situation. I*
19 *mentioned the loss of the business in Poland to a rival. Listening to*
20 *the marketing people I cannot see where we [NDS] have had any*
21 *success. At least part of the problem is the history of the insecurity of*
our technology. P7 to P10 [NDS Smart Cards] were hacked and the
fact was very public knowledge. Now we have the situation in the
USA.

22 *We must face the fact that our [NDS's] reputation is bad and our*
23 *competitors make capital out of it. We can claim that P11 is not*
24 *hacked but how confident we be of the technology. Part of the reason*
25 *that it is not hacked is the difference we have all made. We have*
introduced control [control of the hackers]. The question is whether
the control is camouflaging the weaknesses in our technology. My
fear is that it is.

26 *In listening to Alex [Oliver Kommerling], who is not allowed to hack*
27 *P11 [NDS smartcard], and coupling that with what is said by others I*
28 *fear P11 is as weak as anything else we have produced. If that is so it*
will be hacked as soon as it is used in the USA.

1 . . . The techies must realize that their technology has not been put to
2 the test because largely we are stopping it [by controlling the
3 hackers]. We cannot say the same for any other part of the world;
USA included, where the platform may be used. A hack on P11 would
destroy confidence in NDS.

4 The consequence of not adding a new factor would be the continued
5 hacking of our technology. To the best pirates it is almost too easy [to
6 hack NDS's Smart Cards and Security System]. The technical security
7 holes and mistakes make it possible.

8 The result of more hacks will be a loss of confidence and a loss of
9 business. At present we are not gaining most of the new projects.
10 How long before we actually lose one to a competitor.¹¹ Our jobs are
11 on the line. Maybe not yet but we are vulnerable.

12 130. On or about October 6, 1997, an NDS Memorandum from Segoli to
13 Hasak, Adams, and Norris, copying Gutman, concerning NDS's recruitment efforts
14 of a pirate, Dieter Scheel, and specifically concerning NDS's awareness of
15 Christopher Tarnovsky's identity as "Biggun" on internet piracy websites and chat
16 forums, states:

17 Chris Tarnovsky

18 *When Scheel was in Canada he wrote to Biggun[Tarnovsky] (using*
19 *Anthony's computer and email account) asking for help. At that time*
20 *Biggun wrote back saying that the man behind Marty Mullin's hack is*
21 *named Dieter. It was only after he returned to Germany that Oliver*
22 *[Kommerling] told him that Chris Tarnovsky is Biggun.*

23 *Anthony has told Scheel that Chris Tarnovsky has gone underground*
24 *because he had made promises to the group he was working for and*
25 *could not deliver.*

26 Regarding NDS's possibly hiring Scheel as one of its hacker/agents and giving
27 competitor's ROM Codes to him, the memo goes on to state:

28 . . . he [Scheel] could possibly be of operational interest for us, since
apparently in the narrow world of hackers where there are relatively
few people of true hacking talent, he is a name that people may trust
enough to talk to – perhaps not to give ROM dumps to, but at least to

¹¹ This statement to NDS head of security Reuven Hasak is telling indeed, shedding light on the true motivations of NDS when engaging in the unlawful conduct outlined herein. Specifically, NDS was about to lose an account to a competitor – NDS's biggest account, DirecTV, was on the verge of negotiating a conversion to the conditional access system employed by EchoStar. Accordingly, because its business was "one the line," NDS was forced to turn to unlawful anticompetitive conduct in a last ditch effort to remain afloat in the satellite encryption industry.

1 *talk to . . . He is certainly not on the level of Mike [Tarnovsky] or Alex*
2 *[Kommerling].*

3 131. On or about October 21, 1997, an NDS Memorandum, concerning
4 Tarnovsky using the nickname “Coleman” and NDS’s control over Tarnovsky as
5 one if its hacker/agents, states:

6 *The Coleman alias was used one time and one time only by Mike*
7 *[Tarnovsky] to attack Oliver [Kommerling]. Mike [Tarnovsky] did not*
8 *and does not know about the relationship [between Kommerling and*
9 *NDS] to date . . . The attack was not sanctioned nor done with Roni’s*
10 *[Segoli] nor my [Adams] approval. When I discovered Mike’s*
11 *[Tarnovsky] action I put an immediate stop to this kind of attack.*

12 132. On or about October 22 – 24, 1997, an NDS Memorandum, establishes
13 that John Luyando [nicknamed “Yanni” and “Jellyfish”] was working for NDS as a
14 hacker/agent as early as October 1997 and that NDS concealed to DirecTV that
15 Kommerling was also a hacker/agent employed by NDS. An “urgent” NDS
16 memorandum concerning Kommerling and Luyando was written to Adams
17 indicating that Larry Rissler, Vice President of Signal Integrity for DirecTV, had
18 contacted NDS and was inquiring as to whether Kommerling was working for
19 NDS. Rissler asked Norris about an individual named “Oli K” or “Oliver Kiss.”
20 Rather than being forthright with DirecTV – NDS’s largest client that NDS was
21 fighting desperately to retain notwithstanding DirecTV’s utter disappointment with
22 NDS’s consistently compromised Security System – Norris lied to Rissler in an
23 attempt to conceal Kommerling’s relationship with NDS.

24 133. In an effort to continue to conceal NDS’s relationship with
25 Kommerling, the memo advises Adams that “Oliver [Kommerling] should not
26 travel with luyando in the future. *I prefer all contact (call [sic], email, etc) be*
27 *discontinued at this point but this can not [sic] happen due to Oliver’s*
28 *[Kommerling] standing in the hacker community.”* A follow up facsimile from

1 Adams to Hasak concerning the possibility that DirecTV was setting a trap for NDS
2 hackers Kommerling and Luyando to be arrested when attempting to get onto an
3 airplane, and NDS's actions to circumvent any incrimination of Kommerling,
4 states:

5
6 There would have been absolutely no legitimate grounds for detaining
7 [at any airport because DirecTV had notified authorities to be on the
8 look out for Kommerling] him for a second. Had anyone done so
9 there was a lawyer ready to get him out of trouble. *The only possible
10 evidence that could have ever existed to connect Alex [Kommerling
11 and NDS] to the card [a pirated Smart Card] was what was on his
12 PC. It was wiped clean the same day the card was programmed. As
13 an extra precaution the computer was broken into two parts and sent
14 by two separate courier companies to two separate addresses in
15 Germany. . . . Nothing existed [on the pirated card] technically to
16 connect Alex [Kommerling] to the card in either Canada, the USA, or
17 Germany.*

18
19 134. On or about November 10, 1997, in a letter from Norris to Adams
20 concerning the "batulator" and Tarnovsky's hacking ability and efforts discussed by
21 Gutman in correspondence dated November 6, 1997, Norris states: "*fyi, the
22 'compulator' aka 'batulator' code was reversed by Mike [Tarnovsky] several weeks
23 ago and the heart has been exposed . . .*" At this time, Tarnovsky was an employee
24 and agent of NDS and was acting on behalf of and at the direction of NDS.

25
26 135. On or about November 13, 1997, is *the first reference* that Larry
27 Rissler, Vice President of Signal Integrity for DirecTV, *could locate in his notes to
28 "Mike," one of the names used by John Norris to refer to Tarnovsky. It is Mr.
Rissler's recollection that Norris previously told him that he [John Norris of NDS]
had recruited Tarnovsky to work as a consultant for NDS, and that Norris had
moved Tarnovsky to California.*"¹²

¹² In contrast, Norris was not so forthright with United States Customs agents when Tarnovsky's California home was raided. Specifically, at that time, in an attempt to limit exposure of the NDS/Tarnovsky relationship, Norris informed U.S. Customs officials that: (a) the equipment in

1 136. In or around the end of 1998 NDS employee John Luyando sent a
2 letter to NDS executives Reuven Hasak and Ray Adams concerning Kommerling's
3 recent "visit to Jerusalem," and concerning the criminal elements associated with
4 satellite piracy and his regard for Rupert Murdoch. This NDS report states in
5 relevant part:

6 On Monday morning, Yossi [Tsuria] and I had breakfast with Alex
7 [Kommerling] at the hotel. Yossi was relaxed and talkative, and the
8 atmosphere was very open and, in my opinion, was a good discussion.
9 The discussion was around Boris [Floritic]¹³ and the implications of
10 criminal elements entering this [NDS] arena. The two seem to agree
11 that this was no suicide. *They also said that it does not seem possible*
12 *that a commercial company would take such drastic steps just to save*
13 *its product. (Yossi said: 'There's a limit to how far out I will stretch*
14 *my neck out for Rupert Murdoch')*¹⁴

15 On the issue of Kommerling's dealings for and at the direction of NDS, this NDS
16 report states:

17 Yossi and Alex [Kommerling] also raised a possible scenario, which,
18 to the best of my knowledge, has not been considered. *Alex*
19 *[Kommerling] pointed out that it is very easy to trace the transport of*
20 *Fed-Ex packages or other postal packages.* It would be no problem
21 for a journalist to find that *there have been very frequent exchange*
22 *[sic] of postal packages between Alex [Kommerling] and NDS-UK*
23 *and NDS-Israel. What would happen if a journalist came knocking on*

24 Tarnovsky's home – which included various pirating devices such as a card emulator – was
25 property of NDS; (b) Tarnovsky had been an NDS employee since February 1, 2001; and (c)
26 Customs' officials were not to search Tarnovsky's home without a search warrant.

27 ¹³ Boris Floritic authored a well-regarded research paper on reverse engineering of smart card
28 technology. Plaintiffs are informed and believe that NDS contacted Floritic, whom NDS referred
to as "Tron", regarding reverse engineering smart cards used for conditional access systems
employed by satellite signal providers. In October 1998, Floritic was found dead in a Berlin park
(hanging from a tree with his feet on the ground). Upon investigation, Floritic's father found a
NDS invoice dated July 12, 1998 which read "Hello Boris, here are the analog devices, good
luck."

¹⁴ Rupert Murdoch's News Corp. is the parent company of NDS.

1 *Alex's [Kommerling's] door with a Camera? . . . Yossi said he would*
2 *like a contingency plan developed for such a scenario.*

3 137. On or about May 31, 1999, an NDS Letter was sent from Yehonatan
4 Shiloh from NDS Technologies Israel, Ltd. to the Israeli Embassy regarding
5 satellite pirate “Plamen Donev,” who was well known for hacking NDS’s Smart
6 Cards, and a visit he was making to NDS’s laboratory in Haifa, Israel. The letter
7 states that “*Plamen Todorov Donev [hacker and pirate programmer], (Passport*
8 *number 5389412) [is] employed at NDS Ltd. as Director and Advisor for Technical*
9 *Design and Research.*”

10 138. On or about June 18, 1999, an NDS Letter to Hasak from Adams
11 concerning NDS’s hiring satellite pirates and hackers in order to “CONTROL”
12 them, as well as NDS’s fear of losing its contract with DirecTV to be DirecTV’s
13 smart card provider, states in relevant part:

14

15 *So if a risk existed what were we to do. With Risks we normally*
16 *think of: AVOIDANCE, REMOVE, CONTROL*

17 *We could avoid the risk by not introducing P3. We could*
18 *remove the risk by introducing an un-hackable card. So, we*
19 *are left with CONTROL.*

20 *We decided that the best control was to control the perpetrators*
21 *[pirates and hackers]. To control we decided to recruit, to*
22 *neutralise. The twin advantages of doing this were:*

- 23 1. *to stop them actively hacking P3 on behalf of the Canadians*
24 2. *to learn from the two recruits (referring to Pluto [Plamen*
25 *Donev] and Vesco [Vesselin Nedeltchev]), their methods, and*
26 *preventative measures.*

27 *With the benefit of experience over the next six months you and*
28 *I will be able to talk very convincingly about the cost benefit of*
 our recruitment.

1 The one hostage that we carry into all these deliberations is the
2 weaknesses in our [NDS's] technology [smart cards]. I have
3 not told you before as i assume you already know the same as
4 me. Yossi admits that our cards are even more vulnerable to
5 attack than anyone realised before. Glitching is practically a
6 magic key to access our cards. . . .

7 So given that the technology can be hacked very quickly what
8 do we do. Do we abandon recruitment [of other satellite
9 pirates and hackers] and leave everything to ECM's [electronic
10 countermeasures to fight piracy] in which case we will lose our
11 customers [DirecTV] in a short space of time. Or, do we
12 continue to recruit [hackers]. This gives us time to get the
13 technology correct. Having the enemy [hackers and pirates] on
14 our side removes the complacency element and makes the
15 improvement of our technology a geometric progression.

16 What we need is support. In the main that is money,
17 money, money.

18 Without a realistic budget we cannot recruit the top hackers.
19 They know what they can get from the pirates. We need to
20 control these guys, to pay them well, and get benefit from
21 them.

22 ... JOD was heavily involved in the DTV negotiations. He
23 thinks we will lose them soon. We will lose them quicker if P3
24 if hacked. This must be a major concern.¹⁵

- 25 **1. With the World's Most Infamous Hackers on its Payroll,**
26 **NDS was able to Dictate When its Smart Cards Would be**
27 **Hacked, and Thus Could Make Additional Monies from its**
28 **Customers by Selling ECMs and Ultimately Doing**
29 **Expensive Smart Card Swaps**

30 ¹⁵ Here again NDS acknowledges the fact that it was on the verge of losing one of its largest
31 clients – DirecTV – and that drastic measures were needed to prevent such a loss. However,
32 rather than improve the quality of its encryption technology, NDS opted to continue with its
33 conspiracy to effectuate, and facilitate others in effectuating a wide spread compromise of
34 Plaintiffs' security system to 'level the playing field' in an illegal anti-competitive manner.

1 139. On or about July 11, 1997, an NDS Memorandum, concerning
2 Tarnovsky's and Kommerling's employment with NDS as two of their best
3 hackers, NDS's control over them and its desire to have Kommerling continue to
4 engage in satellite piracy, states:

5
6 *I think we should reflect on what the objective is, either, to get the*
7 *programme, or, to run a complex operation. I feel sure that, for*
8 *understandable reasons, the possibility of looking at alternatives is*
9 *being passed over. Why not for example, let Alex [Kommerling] and*
10 *Mike [Tarnovsky] run together on this one. Why separate them? I am*
11 *prepared to let JN [John Norris] run the operation.*

12 *. . . For some time there has been speculation about Kommerling and*
13 *the fact that he is no longer acting with the pirates. His withdrawal*
14 *from the USA scene will serve to confirm the suspicions. He is*
15 *suppose to be a pirate and should therefore act like one. . . . In one*
16 *simple move we would get the operation moving and protect*
17 *Kommerling from exposure. he [Jan Saggiori] knows that*
18 *Kommerling is with NDS.*

19 140. On or about December 1, 1997, an NDS Memorandum entitled
20 "Operations Security Group" from Gutman to Hasak, Segoli, Adams, and Norris
21 regarding a "Global View - 12/1/97," concerning NDS's placement of Tarnovsky
22 into Ron Ereiser's pirate organization with NDS's full support, states: "*Ron*
23 *Ereiser's Group - hired Tarnovsky to Calgary . . . CT [Tarnovsky] was tasked with*
24 *creating four secure programmer boxes [illegal NDS Smart Card programmers].*
25 *Each member of the group will receive a box, thus enabling the programming of*
26 *more cards and ensuring that if one of them gets caught - the business of selling*
27 *3Ms [DirecTV hack] will continue. " Concerning NDS's technical support for his*
28 *pirating activity, the memo goes on to state "Mike [Tarnovsky] recently visited*
Israel to meet the staff, set working procedures with them and receive tasks"
to assist him with hacking and piracy.

1 141. On or about December 1, 1997, an NDS Memorandum from Norris to
2 Adams, concerning NDS's providing protection for Tarnovsky for his illegal
3 actions in pirating competitors' security systems, NDS's full awareness of
4 Christopher Tarnovsky's illegal acts, and the possibility hacking EchoStar, states,
5 in part:

6
7 *. . . Mike [Tarnovsky] believes that I [Norris] can not protect him in*
8 *Europe for his past deeds (conspiracy?) and, Alex [Kommerling] has*
9 *been raided once – therefore, Mike [Tarnovsky] could be the subject*
of some official covert investigation into his European activities
[illegal satellite piracy and hacking].

10 142. On or about November 27, 1998, a NDS Letter from Adams to Hasak
11 regarding Adams's "Week Report," concerning piracy, NDS's budget, and NDS's
12 purchasing hacks of its own Smart Cards in order to sell DirecTV Electronic
13 Countermeasures and new Smart Cards, among other things. Adams states: "*so this*
14 *again raises the issue of our budget and as I said I think this will become a major*
15 *issue in the next year. The culture at SKY is to cut costs and if there is no piracy*
16 *someone will suggest it, Psst wanna buy a hack.*"

17 143. On or about December 1998, a Letter is sent from Adams to Hasak
18 regarding "Week Report," and concerning Alex [Kommerling] Adams references
19 NDS's secret Black Hat Team, "*. . . you and I believed that Alex [Kommerling]*
20 *was moving into a managerial role and would be a leader of black hat activity*
21 *[illegal hacking and pirating of competitor's access cards]."* Further,
22 concerning Kommerling's role with NDS, and the reason NDS and Kommerling
23 formed the company ADSR, and NDS's hacking of the Galaxy Smart Card,
24 Adams writes:

25 *. . . he absolutely misinterpreted the whole reason we have formed*
26 *ADSR [a company owned 60% by Kommerling and 40% by NDS].*
27 *You and I know that it is to give Alex [Kommerling] a business face*
that will explain to others what he is doing [provide the appearance of
legitimacy].

28

1 It should be a simple task for one of our techies to prove that the
2 Australian Irdeto card is as vulnerable [hack the card] as any in any
3 other country.

4 I can send Prince [an NDS agent] to Australia and he will visit Pirate
5 dealers and get cards direct from them. Even Alex [Oliver
6 Kommerling] and I could go and do it, want to come. I know that
7 Galaxy has been pirated in the past. . . . What we need urgently are
8 some official cards from each of the system, six of each, making 18
9 total so that we can get the pirates to switch them on. This is the
10 easiest way to prove our case. It will also be very effective and
11 untraceable.

12 144. On or about April 30, 1999, an NDS Letter from Adams to Hasak
13 references a meeting that Kommerling had with Canal+, wherein Kommerling was
14 asked about the www.DR7.com [Menard] Hack release. Kommerling was asked if
15 he could do a hack of the "IRDeto" system in Arabia on PANAM SAT channel
16 ART 1, however, unbeknownst to Canal+, the hack of IRDeto was already in
17 NDS's possession. "JR wants Alex [Kommerling] to hack the system but at the
18 same time to provide a fix. So that when the pirate cards are available he will be
19 able to say that Alex 'the technician' can do a fix in 24 hours. . . . What JR does not
20 know is that the hack is already in our [NDS's] possession. You will recall the
21 occasion when I was asked to get software urgently some 3 months ago. I did it
22 and had to pay 10 [10,000 pounds]. Well that software only needs updating with
23 the new keys. :-)"

24 **B. PHASE 2: NDS Turns These Same Pirates on its Competitors,**
25 **Including Plaintiffs, in an Unlawful Attempt to Control the Piracy**
26 **of its Competitors and, Ultimately, Destroy the Competition**

27 **1. Step 1: With the Assistance of Defendant Oliver**
28 **Kommerling, and other Defendants, NDS Built a**
Sophisticated Laboratory in Haifa, Israel, Where NDS
Cracked Plaintiffs' Smart Card and Obtained Their Secret
ROM and EEPROM Codes

1 145. The reason it takes sophisticated technology to perform an invasive
2 attack on Access Cards is that, in order to develop a way to defeat a Security
3 System, an individual or entity must know and understand how the system works.
4 As a result, an individual or entity must have access to the software contained in the
5 Read-Only-Memory (ROM) and Electrically-Erasable-Programmable-Read-Only-
6 Memory (EEPROM) contained in the Access Cards. The software contained in
7 ROM and EEPROM is written in machine language, which is almost impossible for
8 humans to use or understand because it consists entirely of binary digits. The
9 foundry manufacturing the basic component of the Access Cards uses advanced
10 security designs and manufacturing techniques to render the devices tamper proof.

11 146. A hacker wanting to obtain the software from Plaintiffs' Smart Card
12 would have to use a sophisticated laboratory equipped with a scanning electron
13 microscope and/or focused ion beam, among other things. They would then have to
14 analyze the chip under this sophisticated equipment, mapping out the 1s and 0s and
15 then reverse-compiling those numbers to have access to and understand the
16 imbedded software. This also requires the involvement of very sophisticated and
17 highly skilled programmers and engineers.

18 147. Oliver Kommerling testified in the Canal+ case that NDS engineers
19 used his methods for attacking Smart Cards at the Haifa, Israel laboratory to attack
20 Canal+'s Smart Card. Plaintiffs are informed and believe that this same procedure
21 was used on their Smart Cards.

22 148. Plaintiffs are informed and believe that NDS engineers in the NDS
23 facility in Haifa, Israel obtained Plaintiffs' Smart Cards and using some of the
24 techniques described in "Design Principles for Tamper Resistant Smartcards"
25 written by Kommerling and Markus Kuhn, were able to physically extract the
26 Plaintiffs' code embedded in their smart cards.

27 149. Plaintiffs are informed and believe that NDS engineers disassembled
28 and analyzed the extracted machine code and were then able to explore methods by

1 which people would be able to circumvent the security measures contained within
2 that machine code.

3 150. Plaintiffs are informed and believe that NDS and its employees and
4 agents cracked Plaintiffs' Security System (and made an unauthorized and
5 impermissible copy of the proprietary information contained therein) at the Haifa,
6 Israel facility and transmitted the results to NDS hacker Christopher Tarnovsky in
7 the State of California. One of Tarnovsky's tasks was to distribute this information
8 in a manner designed to proliferate Pirated Access Cards and other circumvention
9 or signal theft devices designed to enable users to illegally modify or alter EchoStar
10 Access Cards and/or Plaintiffs' Security System which could provide unauthorized
11 users to access to EchoStar Programming services on the DISH Network.

12 151. Based upon information and belief, NDS, at its laboratory in Haifa,
13 Israel, (1) intentionally accessed the microprocessor of the EchoStar Access Cards
14 without authorization, (2) physically extracted Plaintiffs' secret ROM Code
15 contained therein without authorization, (3) distributed Plaintiffs' secret ROM
16 Code to Tarnovsky with instructions for its dissemination, and (4) controlled the
17 design, manufacture, and sale of Pirated EchoStar Access Cards and other
18 circumvention or signal theft devices designed to enable users to illegally modify or
19 alter EchoStar Access Cards and/or Plaintiffs' Security System without
20 authorization. NDS orchestrated this plan with the intent to defraud EchoStar of
21 revenue from DISH Network subscriptions and to injure the effectiveness of
22 Plaintiffs' Security System. Defendants' improper motivation for engaging in this
23 illegal anti-competitive conspiracy consisted of, among other reasons, a last ditch
24 effort to retain the business of DirecTV, one of Defendants' largest accounts, who
25 was on the verge of entering into contractual relations with Nagravision in an effort
26 to obtain a more secure conditional access system to protect its satellite signal from
27 unauthorized reception and decryption.

28

1 152. In order to circumvent the Security System, NDS used information and
2 technology in their possession, including but not limited to sophisticated equipment
3 such as scanning electron microscopes and focused ion beams, to access the
4 microprocessor contained on legitimate EchoStar Access Cards. In accessing the
5 microprocessor, Defendants, and those associated with them, obtained and altered
6 valuable proprietary software and information concerning Plaintiffs' Security
7 System that NDS was not entitled to obtain or alter.

8 153. Once NDS obtained the encryption technology and related software
9 code from the microprocessor, they replicated and modified the encryption and
10 other software to interfere with the communication between the Access Card
11 microprocessor and the set-top box that, in the ordinary course of its operation,
12 authenticates which DISH Network programming services legitimate subscribers
13 are entitled to view.

14 154. On or about November 29, 1999, a NDS Memorandum from "Mike"
15 [Tarnovsky] reporting to NDS on the meeting Tarnovsky set up with Hannibal
16 [Saggiori] in order to gather information for NDS concerning the Canal+ and
17 EchoStar hacks, without Saggiori knowing Tarnovsky's purpose. Saggiori asked
18 Tarnovsky who Tarnovsky worked for, and Tarnovsky falsely responded, "*I*
19 *responded about working for 'Flagship Automation from Nashua, NH' as their*
20 *fielded tech-support lead for WonderWare, Inc. I explained how we called the tool,*
21 *'UnderWare' instead and that it is a Windows hosted scripting language/gui*
22 *program . . .*" when, in fact, Tarnovsky was actually working for NDS and had been
23 since approximately 1997.

24 155. Concerning the EchoStar hack, Tarnovsky's Memorandum states:
25 "*Hannibal [Saggiori] believes Alex [Kommerling] is working with the Canadians*
26 *on the E* hack. I explained to him that the Canadians who are behind the hack. I*
27 *told him Discount [Dawson] and Kerrobert Satellite [Ereiser] hated Alex*
28 *[Kommerling] because he did not return nor help them with the 3 VideoCipher II*

1 Plus. I told him that due to this condition, it is unlikely Alex [Kommerling] is
2 behind the E* break. I tried to make him rethink his assumptions on Alex
3 [Kommerling] by use of the Canadians which does seem to have worked, however
4 Hannibal [Saggiori] still believes the IRDeto and SECA [Canal+ 's Code] are
5 Alex's [Kommerling's and NDS's] doing."

6 156. On or about May 5, 2000, an NDS Memorandum captioned "Report
7 Week 18", concerning NDS agent Christopher Tarnvosky and the EchoStar hack,
8 states in relevant part: "You will note that suspicion has fallen on MIKE
9 [Tarnovsky]. This is because, as Hannibal [Saggiori] says, MIKE [Tarnovsky] was
10 the person who introduced the Bolgers [hackers Plamen Donev and Vesselin
11 Neldechhev] to the American/Canadian Pirates. Yet Hannibal [Saggiori] is the one
12 named [in a lawsuit by DTV/NDS]. Thus Hannibal [Saggiori] concludes that MIKE
13 [Tarnovsky] works for NDS. There are a series of threatening statements inasmuch
14 that MIKE [Tarnovsky] is behind DR7 [Allen Menard and the website
15 www.dr7.com] and MIKE [Tarnovsky] hacked ECHOSTAR"

16
17 **2. Step 2: NDS Had to Provide the Illegally Obtained ROM and**
18 **EEPROM Codes to a Software Engineer Capable of**
19 **Reprogramming Smart Cards**

20 **a. NDS Used its Employee and Infamous Hacker, Tarnovsky to**
21 **Reprogram Plaintiffs' Smart Cards Once NDS had Illegally**
22 **Obtained Plaintiffs' Secret ROM and EEPROM Codes**

23 157. On or about November 19, 1995, Tarnovsky sent an email to a "Tv-
24 Crypt" pirate list group concerning Tarnovsky's desire to begin hacking smart
25 cards, where he admits his status as a pirate and hacker: "[m]y name is Chris
26 Tarnovsky! I am a hacker/programmer very much into Electronics/Ham
27 Radio/Modems/Video Access Control (!) and anything else out there I find
28 interesting." Tarnovsky's telling email further states, "I am a fanatic when it comes
to Sky . . . Eagerly awaiting tearing into the code for the card! Currently, I am

1 *studying EuroCrypt . . . D2Mac. While waiting for someone else to crack the card*
2 *open.*”

3 158. Further solidifying his status as a hacker and pirate as early as 1995, on
4 or about November 26, 1995, Tarnovsky sent an email to tv-crypt@ghost.sm.dsi
5 concerning “D2Mac Rendezvous,” wherein he requests assistance in hacking a
6 smart card, “*Is there anyway to ‘find’ the keys to it [the smart card] via instructions*
7 *or anything w/o etching it [the smart card] open . . . Any help is greatly*
8 *appreciated . . .*”

9 159. On or about July 11, 1996, Tarnovsky sent an email to Jan Saggiori
10 concerning Tarnovsky’s and Saggiori’s combined efforts to pirate Smart Cards.
11 Concerning Tarnovsky’s employment at “ULVAC” at the time, and the equipment
12 at his disposal to hack Smart Cards, Tarnovsky states: “*We [ULVAC] also have an*
13 *E-beam tester downstairs . . . everything will be fine here once I am settled in*
14 *place! For now, nothing for that [hacking] is possible. I am waiting for things to*
15 *become “more comfortable” (!) ... Now, we need to find the SA for the CTV stuff*
16 *and the old CANAL+/CINECINEMAS keys [secret keys to EEPROM or ROM] . . .*
17 *we want everything! . . . – Chris”*

18 160. Chris Tarnovsky would later become a full scale satellite hacker and
19 pirate and would begin posting illegal keys and information under many nicknames
20 as alleged herein, in order to facilitate and assist in the hacking of Plaintiffs’
21 Security System.

22 161. On or about November 29, 1998, a post to the Internet by “Nipper”
23 [Tarnovsky] indicating his full understanding of the illegal activity engaged in by
24 stating, “*EVERYONE BE VARY WEARY OF PEOPLE WHO PLAY STUPID*
25 *INSIDE THIS CHAT ROOM! SOME WILL MOST LIKELY TURN OUT TO NOT*
26 *REALLY BE WHOM THEY SAY!”*

27 162. In or about March 1999, Tarnovsky’s relationship with NDS did not
28 appear to have changed as John Norris and Tarnovsky attended the SBCA show in

1 Las Vegas, Nevada. Norris introduced Tarnovsky under the NDS alias “Mike
2 George,” and Norris claimed Tarnovsky was his nephew.

3 163. On or about July 23, 1999, Tarnovsky sent an email from
4 epr126@webtv.net to Alan Guggenheim, President of NagraStar at
5 guggenheim@nagra.com wherein Tarnovsky openly acknowledges the injurious
6 effects of the NDS conspiracy, and his intention to continue to hack NagraStar
7 Smart Cards: “*After a visit to your web site <http://www.nagra.com>, we noticed that
8 the information about the Echostar Corporation is outdated. We would greatly
9 appreciate if you updated the subscriber count to 2.5 million + 50000 pirate
10 customers. Best Regards, The Swiss Cheese Production [Tarnovksy].*”

11 164. On or about December 7, 1999, a post to the Internet by “Shrimp”
12 [Tarnovsky] concerning Tarnovsky’s knowledge of reverse engineering Smart
13 Cards and the cost of doing so, he states “*any chip can be reverse engineered to the
14 point of understanding for under \$110,000. The problem is they might be more
15 devices which would need to be reversed and then the costs mount up.*” A post later
16 this date by “GS2” affirms the relationship between Chris Tarnovsky and Al
17 Menard and states that “*Shrimp [Tarnovsky] is a very good friend of DR7
18 [Menard].*”

19 **b. NDS Considered Other Alternatives and Approached**
20 **Other Well-Known Hackers in Their Decision to**
21 **Compromise Plaintiffs’ Security System and**
22 **Disseminate Plaintiffs’ Proprietary Codes**

23 165. In or around August 1997, NDS employee and agent Oliver
24 Kommerling, acting under the direction and control of NDS, contacted a then
25 current satellite hacker Marty Mullen. During this conversation Kommerling,
26 acting on behalf of and at the express direction of NDS, advised Mullen that if he
27 would delay in releasing hacking software related to NDS’s H-Card that
28 Kommerling was authorized to offer Mullen the DISH Network hack. In fact,

1 Kommerling informed Mullen that EchoStar's code was in the process of being
2 extracted at a *highly sophisticated* laboratory in Europe. Plaintiffs are informed and
3 believe that Kommerling was referring to NDS's matam lab in Haifa, Israel which
4 Kommerling assisted NDS in developing and that the authorization referred to by
5 Kommerling came directly from NDS.

6 166. Plaintiffs are informed and believe that, prior to obtaining the help of
7 Tarnovsky, Menard, Dawson, Koin, Frost, Sergei and Quinn, among others, NDS
8 considered other methods of disseminating the codes, fixes, patches, software,
9 support and other information necessary to accomplish the widespread compromise
10 of Plaintiffs' conditional access system. Specifically, in sworn affidavit testimony
11 obtained from Martin Paul Stewart (f/k/a Martin "Marty" Mullen), Mullen testifies
12 as follows:

13 In August 1997, I was contacted via telephone by an individual named
14 Oliver Kommerling ("Kommerling"). During this conversation,
15 Kommerling introduced himself to me and informed me that he would
16 soon be in possession of the first hack of the EchoStar/NagraStar
17 ROM Code. Kommerling stated to me that this ROM Code was
18 currently being extracted in a "highly sophisticated laboratory in
19 Europe." Kommerling then informed me that he was able to offer me
20 the hack on the EchoStar/NagraStar microprocessor and that he
21 wanted to come to Canada and arrange a meeting to discuss the
22 details. Kommerling said that he was informed that I was in
23 possession of pirating software for the DirecTV H-Card and that if I
24 delayed in releasing that software he was authorized to provide me
25 with the DISH Network ROM Code. It is my understanding, after
26 speaking with numerous individuals including, without limitation,
27 Kommerling's agent John Luyando ("Luyando" or "Yanni"), as well
28 as reading Kommerling's sworn declaration filed in support of the
Canal+ litigation against NDS, that at the time Kommerling contacted
me and stated that he would provide me with the soon-to-be-
completed EchoStar/NagraStar ROM Code extraction, Kommerling
was an NDS employee and was acting on behalf of, and under the
direct control of, NDS.

Mullen Affidavit ¶ 16 (emphasis added).

1 In February 1998, Kommerling contacted me again via telephone and
2 advised me that the DISH Network hack had been completed and that
3 the DISH Network ROM Code had been fully and successfully
4 extracted from the EchoStar's Access Card's microprocessor.
5 Kommerling further told me that "Yanni" would be contacting me
6 within the next couple of weeks to set up a meeting in Canada to
7 discuss Kommerling's authority to offer me DISH Network's ROM
8 Code. During this conversation, Kommerling stated that he was also
9 able to provide me with support for the DirecTV H-card hack in
10 addition to providing us the DISH Network ROM Code, as long as I
11 delayed in releasing any software for the DirecTV H-Card.

12 Mullen Affidavit ¶ 21 (emphasis added).

13 In accordance with Kommerling's statements to me, "Yanni" called
14 me in early March of 1998 and arranged a meeting to discuss
15 Kommerling's offer of the DISH Network ROM Code. This meeting
16 took place on Friday, March 13, 1998 at the Hilton hotel in Windsor,
17 Ontario. Persons in attendance at this meeting with Luyando
18 ("Yanni") included myself, Archie Timuik, and Joseph Lucker.
19 "Yanni" informed us that Kommerling could not be in attendance at
20 the meeting because of work conflicts, but that Kommerling had
21 bestowed full authority on "Yanni" to negotiate Kommerling's offer
22 of the DISH Network ROM Code.

23 Mullen Affidavit ¶ 22 (emphasis added).

24 During this meeting, "Yanni" informed us that Kommerling was
25 authorized to offer us the DISH Network ROM Code for \$1,000,000
26 USD. During this March 13, 1998 meeting, "Yanni" informed us that
27 Kommerling was willing to either set up a demonstration of the DISH
28 Network hack, or provide us with a portion of the DISH Network
ROM Code so that we could verify that Kommerling was, in fact, in
possession of the hack.

Mullen Affidavit ¶ 23 (emphasis added).

Because we were unwilling to provide Kommerling with the entire
\$1,000,000 USD upfront, negotiations came to an end. Shortly
thereafter, I learned through common knowledge in the satellite
pirating community, as well as through Al Menard's www.dr7.com

1 website and Chris Tarnovsky's postings on same, that this DISH
2 Network ROM dump had been provided to another group known as
3 the "Swiss Cheese" Group.

4 Mullen Affidavit ¶ 26 (emphasis added)

5
6 **c. NDS and Tarnovsky Designed and Built the "Stinger"**
7 **that Tarnovsky and Allen Menard Used to Monopolize**
8 **the Sales and Distribution of the "EchoStar Hack"**
9 **over the Internet with the Secret Information Illegally**
10 **Extracted EEPROM and ROM of Plaintiffs' Security**
11 **System**

12 167. In or about 1999, Defendant Menard, owner and proprietor of the
13 www.DR7.com website, became the first person to possess a device that could
14 reprogram Plaintiffs' Access Cards so that they would provide unauthorized access
15 to the DISH Network's Programming. NDS provided Menard this initial
16 reprogrammer via Tarnovsky. With the assistance of NDS, Tarnovsky was able to
17 develop, design and create this reprogrammer which he coined the "stinger."

18 168. Menard was the only person to possess such a device for
19 approximately a year and a half, or from 1999 until early 2001,¹⁶ and thus, with the
20 assistance of Tarnovsky and NDS, was the only person who had the ability to alter
21 or modify Plaintiffs' Access Cards, besides NDS, so that they would provide
22 unauthorized access to DISH Network's Programming.

23 169. The initial monopoly in the production of altered Access Cards set up
24 by Tarnovsky and Menard with the assistance and knowledge of NDS was unique.
25 Generally speaking, the original developer of a method or device designed to
26 circumvent video encryption technology tries to get as much cash as possible by

27 ¹⁶ As a result of Tarnovsky's December 23 and 24, 2000 postings, satellite pirates and software
28 engineers around the world were then able to design and build their own card reprogrammers
thereby exacerbating the piracy of Plaintiffs' signal.

1 selling the method or device to multiple sources. Menard's situation is, in Plaintiffs'
2 knowledge, the only time in the history of satellite and cable piracy where the
3 developer of a method or device designed to circumvent video encryption
4 technology worked with only one outlet source. Plaintiffs are informed and believe
5 that the NDS controlled Tarnovsky and Menard's distribution model which was
6 designed and implemented by NDS in accordance with NDS's overriding plan to
7 "CONTROL" the hacks of both DirecTV and NDS's competitors conditional
8 access systems.

9 170. NDS, directly and through its employees and/or agents, provided
10 Tarnovsky and Menard the information necessary to accomplish the acts
11 complained of herein with such information being sent by NDS to Tarnovsky in the
12 State of California, and then, pursuant to NDS's instruction, from Tarnovsky to
13 Menard in Canada.

14 171. On or about November 11, 1998, a post to the Internet by "Nipper"
15 [Tarnovsky] on www.dr7.com website, concerning a threat by Tarnovsky of his
16 alleged ability to dump the contents of the Plaintiffs' smart card, states: "we are
17 able to also dump the contents of this card [Plaintiffs'] as well. What is it exactly
18 the fine people of our country wish for? Christmas is coming my fellow Canadians!
19 PS. Coming soon, Charlie [Referring to EchoStar's CEO Charlie Ergen],
20 >Nagravision construction set=@

21 172. On or about November 12, 1998, a post to the Internet by "Nipper"
22 [Tarnovsky], concerning pirating and hacking the EchoStar system, states: "ALL
23 THESE ROUTINES WRE ALMOST DIRECT TRANSLATIONS FROM THE
24 ROM [Read Only Memory]. THE 2 TABLES ARE USED IN THE REAL CARD
25 AND WE SIMPLY PORTED THE CONVERSION OF THE REFERENCE INTO
26 THE BLOCKER. NIPPER THE BUTTLICKER= IS ALSO THEIR TEXT. IN THE
27 CAM DUMP, WE SIMPLY SHOWED YOU WHERE KEYS WERE LOCATED.
28

1 NOTE THERE ARE 2 POSSIBLE CHANNEL DECRYPT KEYS USED. OFFSETS
2 28h AND 30h (KEYS FLOW IN ORDER). ENJOY!@

3 173. On or about November 20, 1998, a post to the Internet by “DR7”
4 [Menard], concerning additional files and assistance for the EchoStar hack, states:
5 “a file was sent too me recently by Swiss cheese boys [Tarnovsky] and they asked
6 me too add, lins too it are in todays news 11.20.98 and it is also added to the
7 Echostar tools section... thanks again to the Users of this forum who have
8 contributed their time to the Echostar Project as well as the SCP [Tarnovsky] for
9 initiating this...good luck guys and hope to have more info shortly.” The above-
10 referenced file is the rev 0.52 code which was, in fact, posted and made available
11 on “DR7’s” [Menard’s] website. A later post on this date by “Stuntguy” comments
12 on the inner workings of the Plaintiffs’ ROM Code, but states “unfortunately, until
13 I’ve got a ROM dump¹⁷ [an actual post of Plaintiffs’ ROM Code], it’s all just
14 guesses.”

15 174. On or about November 26, 1998, a later response post to the Internet
16 by “Nipper” [Tanovsky] continues his facilitation of piracy of Plaintiffs’ Security
17 System, states: “REV 052 WILL ONLY COME VIA 288-01 ISSUED CARDS WHOS
18 ATR READS A 60H INSTEAD OF 64H IN ATR BYTE 9.” “Nipper” [Tanovsky]
19 later the same date posts the following “REV052 CARDS DO NOT HAVE ANY
20 UPDATES WAITING IN IRD FOR THEM. ONLY ROM3 CARDS. ROM 2 AND
21 ROM 3 ARE VERY DIFFERENT. THE EEPROM OF REV052 WAS
22 INCORPORATED INTO ROM 3 LEAVING MORE ROOM.”

23 175. On or about December 4, 1998, a post to the Internet by “Nipper”
24 [Tarnovsky] providing the following of Plaintiffs’ codes/keys in response to a
25 request to create a channel list of known tier packs: “RETURN 00 00 03 E7 INSIDE
26 A CHANNEL SERVICE POLL. OPENS THE WORLD UP TO A CARD.”

27
28 ¹⁷ See Footnote 6 Supra.

1 176. On or about December 5, 1998, a follow-up a post to the Internet by
2 “Nipper” [Tarnovsky] states: *“TO CLARIFY THE ABOVE: SEND THIS IN*
3 *RESPONSE TO 20 SUB 08. 01 01 00 00 00 00 00 00 00 0D 81 4C 21 4C 21 00*
4 *00 03 E7 80 09 FF 00 FF 00. AFTER 4C 21: 00 00 (MIN CHAN 000) 03 E7*
5 *(MAX CHAN 999).”* Tarnovsky further clarifies his post by stating *“THE TIER*
6 *MUST BE PLACED INSIDE PIECE OR NOTHING. THE GUIDE IS OPENED*
7 *NOW.”*

8 177. On or about December 7-8, 1998, a post to the Internet by “Nipper”
9 [Tarnovsky] supplying the following illegally obtained information concerning
10 DISH Network: *“21 POLLS OF RELEVANCE: 01: IRD INFORMATION*
11 *(ZIPCODE, TZ, IRD#, IRD INFO) 08: PURCHASED SERVICES; 0B:*
12 *PURCHASED PPV'S. NOTE: 11 IS IRRELEVANT AND IS ONLY FOR*
13 *CALLBACK INFORMATION AND NAGGING. 0B IS WHERE THE ENABLE OF A*
14 *PPV IS COMING FROM.”*

15 178. On or about December 11, 1998, a post to the Internet by Nipper
16 [Tarnovsky] stating: *“THE KEY IS USED TO ENCRYPT CONTROL WORDS*
17 *BACK TO THE IRD INCASE OF OUTSIDERS EAVESDROPPING ON THE*
18 *COMMUNICATIONS AND PREVENTING MULTIPLE USERS RUNNING FROM*
19 *ONE MASTER WITH MULTIPLE SLAVES.”*

20 179. On or about April 6, 1999, a post to the Internet by “StuntGuy” states
21 that *“the one thing we really need in order to accomplish [a long term solution to*
22 *hacking EchoStar] is a ROM dump of the card, because without knowledge of how*
23 *the card works, deep down, we're basically just left flapping in the breeze...E* can*
24 *update the keys all they want, and the 3M'd cards will take the updated keys, and*
25 *everything will be jolly.”*

26 180. On or about December 9, 1999, a post to the Internet by “Shrimp”
27 [Tarnovsky] states *“what did I say about this 'let the kys come in' blocker? The*
28 *only blocker is the original one that blocks all emm's.”* A later post to the Internet

1 by “Shrimp” [Tarnovsky] states “when you ‘hack’ something, you take it in steps.
2 Anything created by man will and can be deconstructed by man.”

3
4 **3. Step 3: NDS and Defendants’ Conspired to Place Plaintiffs’**
5 **Pirated Smart Cards into the Illegal Black Market in a**
6 **“Controlled” Manner**

7 **a. NDS, through its Employee Christopher Tarnovsky**
8 **and other Defendants, Including Allen Menard,**
9 **Created a Distribution Network for Plaintiffs’**
10 **Cracked Security System, Pirate Devices, and Illegally**
11 **Altered Smart Cards**

12 181. With the assistance of NDS by way of, among others, Tarnovsky,
13 Menard produced altered Access Cards using a machine known as a Reprogrammer
14 to place the Access Card microprocessor in a mode that permits reprogramming.
15 NDS provided Menard this initial reprogrammer via Tarnovsky. With the assistance
16 of NDS, Tarnovsky was able to develop, design and create this reprogrammer
17 which he coined, the “stinger.” Menard then loaded the modified software
18 described above, containing programs, information, codes, or commands onto the
19 Access Card, which when re-programmed in this fashion permits access to DISH
20 Network programming services by unauthorized users. None of which would be
21 possible without NDS initially cracking the Security System and providing the
22 proprietary information to Menard through Tarnovsky. Tarnovsky was directed by
23 NDS to provide the information to Menard.

24 182. In so doing, NDS initially, and Menard with the reprogrammer
25 provided by Tarnovsky, effectively damaged the Access Card by impairing the
26 integrity or availability of the data, program systems and information placed on the
27 microprocessor and in associated memory by Plaintiffs to implement the
28 conditional access system for the DISH Network.

1 183. From 1999 to early 2001, Menard used retail sales outlets over the
2 Internet to distribute Pirated EchoStar Access Cards and other circumvention or
3 signal theft devices designed to enable users to illegally modify or alter EchoStar
4 Access Cards and/or Plaintiffs' Security System. These retail outlets were operated
5 as websites including, but not limited to: www.discountsatellite.com and
6 www.DSScanada.com ("Discount Satellite"), owned and operated by Defendant
7 Dawson; www.koinvizion.com ("Koinvizion"), owned and operated by Defendant
8 Sergei; www.hitecsat.com ("Hi-Tec Satellite"), owned and operated by Defendant
9 Quinn; and www.thenewfrontiergroup.com a/k/a the "Blazer Group," owned and
10 operated by Defendant Stanley Frost.

11 184. Advertisements and "links" to these retail outlet sites were placed on
12 Menard's website, www.dr7.com. Menard's website also maintained chat forums
13 and message boards where other pirates and hackers could discuss and share
14 information about the theft of DISH Network programming services and the
15 alteration and modification of EchoStar Access Cards and other circumvention or
16 signal theft devices designed to enable users to illegally modify or alter EchoStar
17 Access Cards and/or Plaintiffs' Security System to facilitate such theft.

18 185. Through Menard and his dealers' websites, and the NDS/Tarnovsky
19 distribution network, satellite signal "pirates" obtain EchoStar Access Cards and
20 alter them in a manner to circumvent Plaintiffs' Security System. Specifically,
21 satellite signal pirates alter Access Cards to interfere with the communication
22 between the Plaintiffs' microprocessor on the Access Card and the IRD that
23 ordinarily authenticates the programming services that the subscriber is entitled to
24 view. As a result, Pirated EchoStar Access Cards, when inserted into an IRD, will
25 cause the IRD to descramble the satellite signal and permit access to EchoStar's
26 Programming services on the DISH Network without payment of the subscription
27 fees or other fees ordinarily required to obtain the right to view such Programming
28 from EchoStar.

1 186. With the assistance of NDS, its agents and employees, Menard and his
2 distribution chain actively marketed these altered Access Cards for the specific
3 purpose of enabling their customers to circumvent the protection of copyright
4 owners' rights and the rights of owners of protected works, which were
5 implemented through the DISH Network subscription process. Moreover, such
6 circumvention of DISH Network's conditional access system allowed the pirates'
7 consumers to avoid paying the ordinary subscription and use fees charged for DISH
8 Network services.

9 187. On or about January 3, 1997, Menard sent an email to Saggiori,
10 concerning Saggiori being the person who introduced Menard to Tarnovsky,
11 wherein Menard states, "*you introduced me to Chris . . . Things have been going
12 great and Chris is a cool dude. Thanx 10000000 tomes over for introducing him to
13 me.*" Menard also informs Saggiori of Menard's new web site www.DR7.com, and
14 states that "All of the most current files [illegal files that enabling pirating smart
15 cards] are now available there." Menard further states that "DR7" is his nickname
16 on IRC.

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

22 189. On or about January 29, 1997, Tarnovsky sent an email to Reg
23 Scullion ("Scullion"), one of Tarnovsky's pirate archrivals, threatening Scullion
24 and establishing his relationship with NDS, formerly NDC, wherein Tarnovsky
25 states: "*[i]f I am against you, you will not have happy customers under your side. I
26 give you the tv and I can remove the tv . . . I may just give the source to NDC. I am
27 sure they will purchase it from me and if I agree to stop, then your world stops also
28 . . . You could have been a distro. point for us [distribution point for NDS,*

1 Tarnovsky and Menard] . . . Instead you are a thefe.” Tarnovsky then signs off,
2 “bye! biggun.”

3 190. NDS facilitated Menard and his distribution network in offering the
4 public and trafficking in the altered Access Cards through various websites,
5 including: www.hucardcentral.com; www.discountsatellite.com;
6 www.koinvizion.com; and www.hitecsat.com. On these websites, Defendants, and
7 those acting in concert with them, as a direct result of NDS’s actions of providing
8 Tarnovsky and Menard with the information necessary to alter Access Cards on a
9 large scale, offered:

- 10 a. to sell Pirated EchoStar Access Cards and other circumvention or
11 signal theft devices designed to enable users to illegally modify or alter
12 EchoStar Access Cards and/or Plaintiffs’ Security System that permit
13 unauthorized access to DISH Network programming services;
- 14 b. to perform the service (for a fee) of altering EchoStar Access Cards for
15 members of the public who submit the EchoStar Access Cards through
16 the mail;
- 17 c. to purchase EchoStar Access Cards from members of the public,
18 presumably to permit alteration and resale of the Pirated EchoStar
19 Access Cards for unauthorized access to DISH Network programming
20 services; and
- 21 d. to exchange several deactivated EchoStar Access Cards submitted by
22 members of the public for a Pirated EchoStar Access Card that would
23 provide unauthorized access to DISH Network programming services.

24 191. On or about May 1999, DirecTV raided Scullion’s house in Rigvad,
25 Quebec, Canada. Jim Whalen, a retired FBI Agent employed by DirecTV was on
26 the raid. Whalen observed a handwritten note by Scullion and videotaped it and
27 later had it transcribed. Concerning the illegal pirating activity by Tarnovsky,
28

1 NDS, and Menard, the note stated that Scullion had been contacted by Menard in
2 about April 1999, concerning:

3
4 *As an administrator on his [Menard's] forums [www.DR7.com] he*
5 *[Menard] personally made me aware that he was programming E3M*
6 *cards about April 1999 and wanted to know if Avantec Bahamas LTD*
7 *[one of Scullions d/b/a's] would be interested in carrying this product*
8 *developed by Chris Tarnovsky. He stated that although I had*
9 *previously had many run ins with Mr. Tarnovsky as BG or Big Gun*
10 *that I should not let this be an impediment to good business.*

11 *He [Al Menard] told me [Scullion] at the time that Chris Tarnovsky*
12 *had done this [EchoStar] fix at the request of NDS and that it had their*
13 *sanction and would cause no legal problems.*

14
15 192. A few nights later, he [Menard] actually stated that my selling these
16 [EchoStar hacked cards] could cause me not to be bothered as much by NDS and
17 that he had been assured by Chris [Tarnovsky] that they would look favorably on
18 this and that I would curry favor with them by doing this.

19
20
21
22
23
24
25
26
27
28
**b. Allen Menard Set Up a Distribution Network in a
"Controlled" manner at NDS's Instruction, By Using
Only Five Distributors, Defendants David Dawson,
Tod Dales, Andrei Sergi, Stanley Frost and Sean
Quinn**

193. Satellite pirates use the information produced from NDS's efforts, and provided by NDS and its employees and agents, to access the microprocessor embedded in EchoStar Access Cards and to reprogram individual EchoStar Access Cards and other circumvention or signal theft devices designed to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security System.

194. As a result of NDS's and Defendants intentional acts, and those acting in concert with NDS, pirates have and are actively engaged in the manufacture, import, export, offering to the public, or otherwise trafficking in technological devices and services, including altered Access Cards and Reprogrammers, that

1 permit unauthorized users to access DISH Network programming services without
2 paying subscription and other fees normally charged for such access.

3 195. Through this scheme to create an underground supply of Pirated
4 EchoStar Access Cards and other circumvention or signal theft devices designed to
5 enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
6 Security System, NDS has furthered its intended fraud of facilitating others in
7 obtaining unauthorized access to valuable DISH Network Programming, free of
8 charge. At the same time, Menard and his distribution network were able to, and
9 did, obtain valuable consideration for the Pirated EchoStar Access Cards and other
10 circumvention or signal theft devices designed to enable users to illegally modify or
11 alter EchoStar Access Cards and/or Plaintiffs' Security System they sold to other
12 members of the public.

13 196. In addition to Frost, Sergei, Dawson, Quinn and Dale, Menard also
14 approached Reginald Scullion with an offer to participate in the NDS/Tarnovsky
15 and Menard "CONTROLLED" distribution of the "EchoStar hack" in furtherance
16 of the overriding NDS conspiracy to effectuate and facilitate others in effectuating a
17 wide spread compromise of Plaintiffs' security system. In his sworn Declaration
18 attached hereto, Scullion testifies as follows:

19
20 In or about fall 1998, Al Menard ("Menard"), owner and operator of
21 www.dr7.com, first approached me wherein he informed me that he
22 was involved in a plan to be the Canadian leader in distributing
Pirated EchoStar Access Cards.

23 (Scullion Declaration ¶ 11) (emphasis added).
24

25 On or about April 1999, Menard approached me a second time to
26 solicit my participation in his distribution network to sell Pirated
27 EchoStar Access Cards. During this conversation, Menard informed
28 me that he was "close to receiving a full hack of the EchoStar system"
and, because of the pirate community's past interest in Swiss Cheese

1 Production's products, Menard's distribution plan was a guaranteed
2 money maker. Menard also informed me that the distribution network
3 was going to have something special attached with its operation: the
4 protection and control of NDS. Menard informed me that NDS was
5 the entity whom had ordered the hack and the distribution of Pirated
6 EchoStar Access Cards through Menard's distribution network via
7 Tarnovsky. Menard informed me that NDS had an arrangement with
8 Tarnovsky to provide the support and facilitation of the hacked
9 EchoStar ROM Code to be sent to Menard to be used in the
10 distribution network. Menard also informed me that I had nothing to
11 worry about with respect to being raided by the RCMP due to the fact
12 that NDS would be running interference in the distribution network
13 and that NDS was connected and had a solid relationship with the
14 RCMP.

15 (Scullion Declaration ¶ 17) (emphasis added).

16 197. On or about October/November 1999, Menard contacted Scullion
17 again wherein Menard informed Scullion that the Pirated EchoStar Access Cards
18 were "ready to be distributed to the public." Menard admitted that he had certain
19 vendors already established to distribute Pirated EchoStar Access Cards including,
20 but not limited to, Dawson, Quinn, Sergei, Frost, among others. Menard solicited
21 Scullion to be another one of his network dealers.

22 198. On or about October 7, 1998, an Internet posting by "DR7" [Menard]
23 which is only the half truth, states:

24 *I HAVE NO SOFTWARE FOR A ECHO HACK AND EVEN IF I DID*
25 *IT WOULDN'T BE HERE BECAUSE OF DEALERS [the Distribution*
26 *chain that Menard and NDS controlled] SELLING IT. IF PEOPLE*
27 *(DEALERS) WANT IT SO BAD TAKE THE INFO I PROVIDE AND*
28 *START HACKING...TILL THEN LEARN ABOUT THE SYSTEM.*

29 199. On or about April 20, 1999, Dawson and Discount Satellite were
30 raided in Edmonton by the RCMP after local reports regarding Dawson's selling
31 pirated DSS and EchoStar access cards and other illegal signal theft devices on the
32 Internet through his website, www.discountsatellite.com. Among the items

1 confiscated were illegal satellite access cards, computers, and other equipment used
2 to program access cards, approximately \$69,500 in U.S. and Canadian money
3 orders and cash, and drugs. Notwithstanding the raid on the confiscation of his
4 pirating equipment, Dawson continued to operate his illegal business in Canada
5 through his website, www.discountsatellite.com.

6 200. On or about August 24, 1999, a post to the Internet by "DR7"
7 [Menard] responding to a request by a member that "JD" [Dawson] release the
8 information regarding E3Ms [EchoStar hacked ROM Code] in order to increase the
9 number of [pirated EchoStar Access] cards in the market and provide information
10 to those who can support their own cards with this information. *DR7 [Menard]*
11 *responds by stating that there is one party in control of the E3Ms [NDS] and that*
12 *revealing any information will never happen.*

13 201. 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 ago
15 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] states that he "*confirmed with JD [Dawson] that the*
18 *keys in the latest talk.cfg file are not for AVR freeware and will only work on JD's*
19 *[Dawson's] AVR.*"

20 202. On or about February 2, 2000, Dawson and Discount Satellite were
21 raided a second time by the RCMP after local reports regarding
22 Dawson's continued selling of pirated DSS and EchoStar access cards and other
23 illegal signal theft devices on the Internet through his website,
24 www.discountsatellite.com. On or about early 2000, DirecTV brought suit against
25 Dawson, among other satellite pirates, for selling pirated DSS access cards in the
26 United States wherein judgment was entered against Dawson for \$14.7 million.

27 203. On or about March 29, 2000, DirecTV executed and seized Dawson's
28 business in satisfaction of the judgment obtained by DirecTV against Dawson.

1 Shortly thereafter, Dawson posted a public statement on his website,
2 www.discountsatellite.com, regarding the status of his business's operations.
3 Included in this statement, Dawson provided a link to www.DSScanada.com,
4 another website owned, operated, and maintained by Dawson. Through this
5 website, Dawson continued to solicit business from his large customer base in
6 addition to new customers.

7 204. On or about June 21, 2000, a post to the Internet by "Hitec" [Quinn],
8 concerning "Koin" [Sergei], states "[f]or the time being... I am removing all dealer
9 links from the site... Koin is closing the website but still accepting orders at
10 Koin@koinvision.com . . . now its cash no money orders at all and no site.... I think
11 it was a wise choice for Koin in my opinion. . . . Any other files that are required to
12 help out the Koinster will be posted here from now on."

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

23
24 **4. Step 4: After NDS's Competitors, Including Plaintiffs, Began**
25 **Employing Electronic Countermeasures to Combat NDS's**
26 **Controlled Pirating of their Security Systems, NDS Would**
27 **Completely Destroy its Competition**
28

1 206. Defendants' conduct also gave Defendants and satellite pirates the
2 ability to design, manufacture, and sell Pirated EchoStar Access Cards and other
3 circumvention or signal theft devices designed to enable users to illegally modify or
4 alter EchoStar Access Cards and/or Plaintiffs' Security System for a profit, or to
5 release that information to other pirates for the purpose of allowing them to
6 generate their own Pirated EchoStar Access Cards and other circumvention or
7 signal theft devices designed to enable users to illegally modify or alter EchoStar
8 Access Cards and/or Plaintiffs' Security System.

9 207. Based upon information and belief, NDS committed these acts in,
10 among other places, the State of California, the Country of Canada, and the Country
11 of Israel. Further, through the distribution network set up by NDS using
12 Tarnovsky, Menard, Dawson, Frost, Sergei, Quinn and others, NDS committed
13 these acts throughout the entire United States and abroad by providing the
14 unlawfully obtained proprietary information, codes, fixes, and support, as well as
15 other forms of information and assistance, via the internet.

16 208. On or about September 6, 1999, a post to the Internet by "KamID0"
17 states "you have to remember that when I made the original page (Dec 1998) the e*
18 hacking was in its infancy so entire mains were needed. I could easily make it do
19 what you asked, since I start with a base file then add lines for each of the options.
20 All I would need to do is just put in the keys."

21 209. On or about September 10, 1999, a post to the Internet by "automan,"
22 entitled "key change today this morning," states "*another keychange and my rev2.5*
23 *is alive! You guys rock!*" "Uniwiz" responds by stating "*hehe....better knock on*
24 *wood! I feel an ECM coming.*" "DR7" [Menard] responds by stating "*I agree*
25 *things are going good automan but I think more time is needed to show the problem*
26 *has been fixed.*"

27 210. On or about October 6, 1999, a post to the Internet by "Code"
28 [Tarnovsky], concerning a new circumvention or signal theft device called an AVR,

1 states “if the key servers are working correctly, you will know the new avr key they
2 [DISH Network] are about to switch to in advance!” A later post to the Internet by
3 “JD” [Dawson], on the same date and concerning inquiry to purchase AVR devices,
4 states “we [Defendants] have available to us now an aftermarket avr device that
5 will activate all channels on the Echostar Dishnetwork system. It runs without the
6 use of the original plastic card and is totally supported via the internet. It is NOT
7 an auto-update product and will stop working in the event of a keychange.
8 HOWEVER, key updates are posted within minutes and available to all. . . . Total
9 cost for board and programmer is currently 150.00 usd. Or 110.00 usd for just the
10 avr board.”

11 211. On or about October 6, 1999, a post to the Internet by “DR7” [Menard]
12 states “a key change did occur [from Plaintiffs] and then reverted back to the other
13 one, don’t know why? I imagine we will see the key change tomorrow and they
14 were testing it...”

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

21 213. On or about October 27, 1999, a post to the Internet by “uniwiz” states
22 “lastly, I’m getting the idea that an autoroll product is impossible and/or even the
23 E3M [EchoStar 3M] boys [Defendants/Tarnovsky/Menard] can’t decrypt the
24 stream packets? The latter sounds impossible to me considering NiPpEr’s
25 [Tarnovsky’s] posts.” A later post to the Internet by “uniwiz,” on the same date,
26 states “NiPpEr [Tarnovsky] might have gotten cmd 00 decrypted but he had the
27 cam do it for him? They know what, where, and why, but not how the keys get
28 decrypted from stream?” A later post to the Internet by “DR7” [Menard], on the

1 same date, states *“just because you do not have one auto-updating and because*
2 *people [Defendants/Tarnovsky] don’t post doesn’t mean it aint happening.”* A later
3 post to the Internet by “DR7” [Menard], on the same date, states *“As I’ve told you*
4 *many times and you keep asking over and over like a Dish employee just to make*
5 *sure, the cards are updating without removing from the receiver...how much more*
6 *will it take you to realize this?”*

7 214. On or about October 27, 1999, a post to the Internet by “Code”
8 [Tarnovsky], discussing problems associated with card swap and plans to combat
9 piracy efforts, states *“how do you expect them [Plaintiffs] to swap out when there is*
10 *nothing written to transfer subs? I suppose they’ll send everything down over the*
11 *air to any card you tell them too. I doubt they even have a card ready to be frank.*
12 *If they did, it might even have the same problems they have now inside. The dumb*
13 *thing here is the algorithm they use for encrypting the control words is so huge, this*
14 *means there is no end in sight. They should have used something small and more*
15 *portable. This algorithm alone takes up around 700 bytes of code for someone like*
16 *myself to code (extremely tight). We have seen how they write, it would be 1700*
17 *bytes for them. There goes a chunk of rom/eeprom space just to encrypt control*
18 *words.”*

19 215. On or about October 31, 1999, a post to the Internet by Tarnovsky
20 states *“Echo is in bed with Nagra and will use the same ROM for all their cards*
21 *around the world.”*

22 216. On or about November 5, 1999, a post to the Internet by “Code”
23 [Tarnovsky] states *“there are not key changes [to Plaintiffs’ Security System]*
24 *because this would become part 2 of the system sale. In the event it’s [Plaintiffs’*
25 *Security System] compromised, they need to upgrade the computer software to all*
26 *this scheduling.”* A later post to the Internet by “xyz” states *“I think it is time for*
27 *some good freeware [a dump of the EchoStar ROM Code]. It seems that for some*
28 *reason or another anyone who knows much about e* hack are all helping the JD’s*

1 *[Dawson] in the world to make more and more money.” A later post to the Internet*
2 *by “M_DeRuke” states “Code [Tarnovsky], how much would the ASIC take to be*
3 *reverse engineered?”*

4 217. On or about November 10, 1999, a post to the Internet by “DR7”
5 [Menard] states “*I guess sometimes things are better off not talked about and its*
6 *better for all...for example the auto-roll, the big dealers [in the NDS, Menard and*
7 *Tarnovsky Distribution scheme] will likely be the first target of E* and if they do*
8 *have auto-rolls that’s who they will attack...but whos to say there isn’t 50-100*
9 *auto-roll versions, guess we wont know till it all goes down.” A later post to the*
10 *Internet by “DR7” [Menard] illustrates Menard’s knowledge of the illegality of his*
11 *activity by stating: “Hitec [Quinn] its in the best interest not to reveal any specific*
12 *info’s [illegasl information on the hack of the Plaintiffs’ Smart Card] as we know*
13 *that we have many here fishing for info’s (echostar), its best just to let everybody*
14 *enjoy and let all the others do the yakking and confuse echo even more.”*

15 218. On or about November 19, 1999, a post to the Internet by “DR7”
16 [Menard] provides instructions to remedy problem of member who received an
17 AVR2 [smart card replacement] and programmer [device used to program smart
18 cards or illegal substitute cards] and was unable to load properly. “DR7’s”
19 [Menard’s] instructions include, “*using DOS talk v1.7 and loading the avr2e3m*
20 *[EchoStar] file which allows AVR2 to use the 3M keys from wintalk.”*

21 219. On or about November 26, 1999, a post to the Internet by “DR7”
22 [Menard] commenting on Plaintiffs’ antipiracy efforts, states that the DISH
23 Network “*should not try to combat piracy efforts until they reach 4-6 million subs*
24 *and that by starting too early they are causing themselves problems because their*
25 *anti-piracy efforts are affecting legitimate subs’ cards.” “DR7” [Menard] also*
26 *states that DISH Network “is in a position to play the tough guys and suffer at the*
27 *hands of others smarter [NDS, Tarnovsky and Defendants] than those employed by*
28 *them.”*

1 220. On or about December 11, 1999, a post to the Internet by “Shrimp”
2 [Tarnovsky] states “*E* is not using DES. They are using a ‘DES-like’ algorithm.*
3 *Plain and simple.*”

4 221. On or about December 15, 1999, a post to the Internet by “DR7”
5 [Menard], responding to an inquiry as to whether there are any TSOP programmers
6 [illegal smart card programmers and devices] that people can make themselves,
7 states “*people are better off buying built adapters.*”

8 222. On or about December 17, 1999, a post to the Internet by “Nipper-
9 Clauz” [Tarnovsky], entitled “*Twas the Night Before Christmas,*” provided illegally
10 obtained EchoStar Bat keys. In the same post, “DR7” [Menard] thanks “Nipper”
11 [Tarnovsky] and acknowledges that the chat users appreciate “Nipper’s” help and
12 that “Nipper” is always welcome. “DR7” [Menard] concludes his post with
13 requesting “Nipper” [Tarnovsky] to make it a great Christmas for everyone by
14 providing additional support.

15 223. On or about December 18, 1999, a post to the Internet by “Gadget”
16 thanks “Nipper” [Tarnovsky] for releasing the AVR1 and Bat keys with
17 instructions how to use them to illegal intercept Plaintiffs’ satellite transmissions.

18 224. On or about December 20, 1999, a post to the Internet by “Nipper-
19 Clauz” [Tarnovsky] entitled “*tis the season to be jolly,*” provides additional
20 illegally obtained EchoStar Bat keys.

21 225. On or about December 21, 1999, a post to the Internet by “Nipper-
22 Clauz” [Tarnovsky] entitled “*be merry harry,*” and provides more illegal EchoStar
23 Bat keys. A later post on the same date by “dooby” asks if “*can anybody please tell*
24 *me what the keys Nipper [Tarnovsky] posts are for??*” Another member “jar”
25 responds by stating “*he [Nipper] posted free [illegally obtained] key for E**” and
26 “jar” then republishes the AVR and BAT keys that were originally posted by
27 “Nipper-Clauz” [Tarnovsky].
28

1 226. On or about December 22, 1999, a post to the Internet by “Poser,”
2 responding to post by “Willie Nelson” addressing issues between “freeware” versus
3 “AVR2,” states *“no doubt, Nipper [Tarnovsky] has some association with the*
4 *group [Defendants—WestE3M]”* In a later post on the same date concerning
5 freeware and hacking Plaintiffs’ smart card, “DR7” [Menard] states *“some should*
6 *realize much has been given for free and is still given every so often, hacking and*
7 *stealing from these same people [Defendants] that brought the most technical*
8 *echostar info ever would be wrong and in my opinion would not further the*
9 *freeware movement...this is about hacking the card people not hacking anothers*
10 *[sic] work thinking your some kinda hero...plain and simple your not.”*

11 227. On or about December 28, 1999, a post to the Internet by “smeese,”
12 entitled “why no key change?,” states *“it seems that E* was changing the*
13 *key[conducting Electronic Countermeasures] daily when Nipper [Tarnovsky] was*
14 *releasing them to the public.”* Later posts on the same date confirm amongst the
15 pirates and hackers that there were no key change since December 23, 1999, that
16 the keys still work, and that *“Nipper [Tarnovsky] timed it just perfect.”*

17 228. On or about December 31, 1999, a post to the Internet by “Skydive”
18 republished the keys originally posted by “Nipper” [Tarnovsky] (KEY 0 EA FA C1
19 D9 74 86 5B 86 KEY 1 34 71 AF 84 AB CC 88 01) and “Skydive” states *“try these*
20 *‘thanks to Nipper [Tarnovsky].’”*

21 229. On or about January 5, 2000, a post to the Internet by “blank” states
22 *“will we get the new batt keys or was that just a one time thing from Nipper*
23 *[Tarnovsky].?? Please and thank you Nipper [Tarnovsky], you seem to be the only*
24 *one capable of producing those keys for us...if you have decided not to do them I*
25 *understand, please post they are not available anymore if that’s the case.”*

26 230. On or about January 8, 2000, a post by “ZaperNut” to the internet
27 states *“I would like to personally thank Nipper [Tarnovsky] for a Merry X-mas and*
28 *New Year gift [Nipper’s posting illegal access keys to the internet and facilitating*

1 *piracy of the DISH Network]. It was a delight to have real TV once again. Open a*
2 *Swiss account or something let us all contribute to a worthy one. Again THANK*
3 *you Nipper [Tarnovsky]!”*

4 231. On or about February 25, 2000, a post by “NiPpEr” [Tarnovsky] to the
5 internet states “*HeRe ArE CuRrEnT KeYs [illegally obtained access keys to the*
6 *DISH Network] ReTuRn SoOn ChArLie: 7D,D9,27,FD,0A,F1,9B,ED;*
7 *8C,D5,5C,27,A1,D8,08,E5.”*

8 232. On or about March 24, 2000, a post to the internet by “xbr21”
9 [Tarnovsky] supplies Plaintiffs’ illegally obtained keys posted on dishplex; “*Key*
10 *05: A8 9B 41 5A 62 8C 57 DE; Key 15: 0F 12 95 8E 2E 32 80 73.”* A later post by
11 “Blindman” states “*I guess someone other than the commercial group now can get*
12 *keys.”* “Pasha” responds by stating “*99.9% same group different alias*” and that
13 “*only ONE group know how to do this.”* A later post by “Code” [Tarnovsky] states
14 “*They do NOT all come from the same ROM. Dishnetwork uses ROM2 and ROM3.*
15 *SkyVista, ExpressVu, and ViaDigital use ROM3 only.”*

16 233. On or about August 15, 2000, a post by “HeeD” states “*the group that*
17 *is supporting DN E3M [the illegal DISH Network hack] has proven that they know*
18 *this system inside-and-out. They are not just taking stabs in the dark, or*
19 *speculating about things...they actually know!”*

20 234. On or about August 22, 2000, an internet post by “Lucky555” states
21 “*I’m looking to start on hacking echostar, I currently have a programmer and*
22 *unlooper with an atmel chip programmer on board. I use this on H cards dss.*
23 *What do I need to get to program that 8515 chip and the cam.”* “DJROCK”
24 responds by stating “*the most promising method of open access which is in fact*
25 *presently better then the H card hack is a Dishnetwork smartcard revision called*
26 *E3M [the hack provided by NDS through, among others, Tarnovsky and Menard].*
27 *This process is not free and it is not available by download over the web. You will*
28 *have to go through a dealer. To use such a revision card you must have knowledge*

1 of the target receiver's secret key which is located in a file stored on a TSOP chip
2 inside the receiver. There are three methods to get this secret key: 1) find an older
3 receiver that has never been plugged in and has a functional memory dump, 2)
4 have a company like us pull it from the TSOP chip, 3) have a company like us pull
5 it from a previously or presently married and subscribed smartcard."

6 235. On or about September 8, 2000, a post to the Internet by "DR7"
7 [Menard] stating "I have only honestly patched 3 times in 18 months...where do
8 they get the info they post about E3m [the EchoStar hack by NDS, its agents
9 Tarnvosky, Menard and others] being so bad??...I have had one [ECM] since day
10 one when discount [Discount Satellite/Dawson] began selling and have not needed
11 to be updated 15 times...total updates I have had are 3 and since June 1999 that
12 has cost me approximately 5 minutes of my time spent loading."

13 236. On or about November 16, 2000, a post to the Internet by "DR7"
14 [Menard] states "maybe the E3M Group [EchoStar hacker group] did reverse
15 engineer Echo or they reversed engineered the original group's hack and took
16 some short cuts... An independent person I know [Tarnovsky] tells me that there is
17 not too many different ways to write 3M code on Echo cards. As far as releasing a
18 patch too many people have reported today from different cities of getting cards
19 programmed.. so I would say that it is true.. as far as closing the hole again as I
20 said it was ONLY speculation on my part as to why the cards are withstanding the
21 ECM [electronic countermeasure]..? if that was the case then how could one write
22 a patch to a hole that is closed.. ? open and close?"

23 237. On or about November 16, 2000, a post to the Internet by "DR7"
24 [Menard] facilitating and assisting in piracy of Plaintiffs' Security System stating
25 "Will Riker did you also notice cards that were out of the stream still work? This
26 includes 01 and 02 cards...also if they reload a card without the loop and just the
27 "call 1-800" it is fixed...doesn't even need to be patched I am told but is very
28 dangerous. I highly doubt they [Plaintiffs] re-wrote the whole code in a day. If

1 they have patch then why haven't they released? Instead they are simply reloading
2 and getting rid of nag screen for now but it will return I'm sure and next time kill
3 more cards which nobody as of yet seems can unloop. Try a 002 that wasn't in the
4 stream for awhile and tell me what happens."

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

9 239. On or about December 1, 2000, a post to the Internet by "Kingtut"
10 stating "I just got my cards from koin [Andre Sergi] and it works fine, reset the ird
11 3000 and did check switch and autorolled fine, the 2700 ird it took hours to
12 autorolled!!! But it worked, I'll wait till the nex key update to see how long it will
13 take to autoroll..." A later post by "DR7" [Menard] on the same date states "It
14 appears this time the auto-roll is taking longer on some systems and might even
15 hang the box but it has been working so far for me."

16 240. On or about December 8, 2000, a post to the Internet by
17 "hammertime3m" stating "DR7 is responsible for the E3M [EchoStar hack], he is
18 the only one loading cards, always has been! He bought the product from a group
19 [NDS via Tarnovsky], he established dealers and started loading cards. That's a
20 FACT! . . . Don't you people find it ODD that he never bashed or attacked the
21 E3M once when it was released. Hell, he went as far as promoting it, praising the
22 dealers, defending it when it was ECM'd. . ."

23 241. On or about December 17, 2000, a post to the Internet by "serf123"
24 inquiring as to whether "SOMEONE would actually be able and willing to post the
25 code to the e3m [EchoStar ROM Code]." A later post to the Internet by "Zoomer"
26 states "IF you dont have a Master code you dont have anything, DR7 [Menard] has
27 the Master code, I was there win he got it, 5 year a ago, and the guy [Tarnovsky]
28 up date him all the time. He [Menard] pays up the but for it. If you had \$\$ for it

1 you would had it back then. He [Menard] was the only one that had \$\$ for it. I
2 miss out.”

3
4 **a. On December 23 – 24, 2000, NDS through its Agent
5 and Employee, Christopher Tarnovsky, Posted the
6 Full Text of Plaintiffs’ Secret EEPROM Code on the
7 Internet – Giving ALL Pirates and Hackers Around
8 the World the Ability to Hack Plaintiffs’ Security
9 System, and thus, the Compromise of Plaintiffs’
10 Security System Exploded**

11 242. The December 23, 2000 publication by “Nipper Clauze” [Tarnovsky]
12 on the Pirates Den website was the critical moment when the key to Plaintiffs’ safe
13 of proprietary information contained in its Access Cards and Security System was
14 given to the world. In this publication, “Nipper Clauze” [Tarnovsky] provided a
15 sequence of events and data that enable a less sophisticated pirate/hacker to dump
16 the entire EEPROM Code segment. The result of such dump enabled a
17 pirate/hacker to locate and identify Plaintiffs’ secret “box keys” and secret “decrypt
18 keys.”

19 243. On or about December 23, 2000, a post by “xbr21” [Tarnovsky],
20 responding to invitation by other members wishing “Nipper Clauze” [Tarnovsky]
21 would reappear and provide information, and states “*you want nipper clauze*
22 *[Tarnovsky] here,*” and then states “*there will be no boxes anymore! There will be*
23 *no more fights amongst us. Learn from this and prosper. Works across the*
24 *world! Do the following: get atr, wait 500ms to ensure card is idle. Send this*
25 *packet to 288-02 or equivalent ROM 3 nagra cam! Rx 4+4096 bytes and you have*
26 *entire eeprom. Send this, then rx 4 bytes + 4096 bytes of eeprom.*” The post was
27 signed by “*nipper clause 00*” [Tarnovsky]. This December 23, 2000 post by
28 Tarnovsky provided hackers around the world the ‘road map’ and instructional code
to effectuate a complete dump of Plaintiffs’ entire EEPROM Code. The actual

1 code posted by Tarnovsky has been excluded from Plaintiff's Complaint so as not
2 to republish its proprietary ROM Code.

3 244. A later post by "willdog" states "wow thanks nipper clauze
4 [Tarnovsky] And it works too." A later post by "grasshopper" states "I've got to
5 agree, this is a totally awesome gift to the Dish community."

6 245. On December 24, 2000, a post to the Internet by "Nipper 2000"
7 [Tarnovsky] at 3:26 a.m. publishing the FULL Echo ROM Code on
8 www.piratesden.com, Discussion Forum. "Nipper 2000's" [Tarnovsky's] post,
9 entitled "*tHe ReAl V3 DuMp!*," stating "*tHeRe WiLl bE nO bOxEs aNyMoRe!*
10 *tHeRe WiLl bE nO mOrE fIgHtInG aMoNgSt uS. LeArN fRoM ThIs aNd*
11 *pRosPer. tHiS WiLl Be PoStEd To ALL NeWsGrOuPs ArOuNd ThE WoRiD!*
12 *ThIs Is Dr7'S cOdE (WeSt 3M v3) tHe rEaL sTuFf!!* Tarnovsky then goes on
13 to state: "I wILL dUmP ALL vErSiOnS oF tHe WeSt CoDe LoOk FoR iT hErE!
14 *nIpPeR cLaUz 00*" [Tarnovsky]. The actual code posted by Tarnovsky has been
15 excluded from Plaintiff's complaint so as not to republish its proprietary ROM
16 Code.

17 246. The first harmful effect of Tarnovsky providing this information was
18 that every ROM3 EchoStar Access Card (approximately 7.6 million in circulation
19 at that time) could then be compromised and forced to dump the EEPROM Code
20 segment revealing the location and identity of Plaintiffs' secret "pairing keys."
21 Prior to Tarnovsky providing this information to the world, a full dump of
22 Plaintiffs' EEPROM Code segment had never been done. As a result, a
23 pirate/hacker was now able to personally update a Pirated EchoStar Access Card or
24 signal theft device to comport with Plaintiffs' frequent "pairing key" changes.
25 Before December 23, 2000, a pirate/hacker was dependent on Defendants
26 Tarnovsky, Menard, Quinn, Sergei, Dawson, and Frost, among others, acting under
27 the control and direction of NDS, to either (1) have Nipper [Tarnovsky] provide the
28 new "pairing keys" on pirate websites, or (2) send the disabled Pirated EchoStar

1 Access Card back to the dealers for updating. However, as a result of Tarnovsky's
2 publication on December 23, 2000, hackers around the world now had the
3 information necessary to personally circumvent any future EchoStar pairing key
4 change to a ROM3 Access Card. Users now simply inserted the disabled Access
5 Card into a card reader, perform the sequence of events and data provided by
6 Tarnovsky which would identify the new pairing key change, and update the
7 Access Card with the new pairing keys. After performing these steps, the user's
8 Pirated EchoStar Access Card or other signal theft device was no longer disabled
9 and could once again receive unauthorized access to EchoStar Programming.

10 247. Approximately 24 hours after the EEPROM Code segment dump by
11 Tarnovsky, or about about December 24, 2003, the first harmful effect of
12 Tarnovsky's publication evolved into the outright destruction and full compromise
13 of Plaintiffs' Security System. Given the information Tarnovsky provided, "Johnny
14 ASIC" was able to create and publish a modified version of Tarnovsky's
15 information consisting of another sequence of events and data that a pirate/hacker
16 could use to dump the entire ROM Code segment. The result os such dump enabled
17 the person to possess the intimate personal knowledge of how Plaintiffs' Security
18 System works. As a result of Tarnovsky's post on December 23, 2000, the piracy
19 world was now able to gain access, retrieve, and steal the heart and soul of
20 Plaintiffs' Security System and to dump both the EEPROM Code segment and the
21 requisite Nagra ROM Code segment.

22 248. On or about December 25, 2000, a post to the Internet by "jumpcue,"
23 entitled "dump of e3m [illegally obtained Echostar ROM Code] has message,"
24 stating that the EEPROM Code posted by Tarnovsky contains "nipper is a
25 buttlicker" message.

26 249. On or about December 27, 2000, a post on www.piratesden.com by
27 "xbr21" [Tarnovsky] stating "*Hate HU, only one of the groups I think west has that*
28 *ST Micro Library ROM, only a few bytes have been released. But I think we got*

1 *enough info thanks to this buffer overflow trick a write hold should be trivial to*
2 *some: \$0000-\$001F Peripheral registers; \$0020-\$003F General-purpose RAM;*
3 *\$0040-\$007F Stack; \$0080-\$021F General-purpose RAM; \$2000-\$3FFF ST Micro*
4 *library ROM; \$4000-\$7FFF User ROM (EchoStar main code); \$E000-\$EFFF*
5 *EEPROM.”*

6 250. On or about December 28, 2000, a post to the Internet by “uniwiz”
7 *provided a list of EchoStar data information and giving thanks to “Nipper”*
8 *[Tarnovsky].*

9 251. On or about December 29, 2000, a post to the Internet by “hitek” [Sean
10 Quinn], entitled “e3m cards,” states “*the new group wants to sell the machines now.*
11 *We do not want to directly sell them, but if you are interested in one, please e-mail*
12 *us and we will give you info on the machines as well as where you can order it*
13 *from. Information is not illegal and support for the machine will be through the*
14 *new group and not us. They have 30 machines ready to go.”*

15 252. On or about May 31, 2001, a Pirates Den “DISH Network” File Search
16 yielded the following downloadable illegal files related to circumvention of
17 Plaintiffs’ Security System in order to receive the unauthorized viewing of DISH
18 Network programming services:

- 19 1. sorry Charlie 2.8 (sc28.exe)
- 20 2. 2 Piece AVR (2pieceavr.zip)
- 21 3. msg306src (mcg306src.zip)
- 22 4. EEEedit (eepedit.zip)
- 23 5. Mracttv2 (mracttv2.zip)
- 24 6. Nagra Blocker (nagra_blocker21.zip)
- 25 7. Rom2 Disassembly (rom2.zip)
- 26 8. Talk10 (talk10.zip)
- 27 9. Dish500 (dish500.zip)
- 28 10. Edit305 (edit305v1.zip)
11. Virgin Bin (virgin.zip)
12. Stuntguy’s NagraVision hacking FAQ
(erom_faq_012000.zip)
13. E3m Disassembly (e3ms.zip)

- 1 14.288-02 disassembly (disasm.zip)
- 2 15.Simple ATME: Programmer \$5 in parts (13418eprog.zip)
- 3 16.Wbininfo150 (wbininfo150.zip)
- 4 17.Dish 3m (dish3m.zip)
- 5 18.Sorry Charlie (sorrycharlie.zip)
- 6 19.Talk 31d (talk31d.zip)
- 7 20.01-02 Dumps (0102dumps.zip)
- 8 21.Talk3.1b (talk31b.zip)
- 9 22.Fbprg16 (fbprg.zip)
- 10 23.Dish Blank Bin (dishblank.zip)
- 11 24.Dish PPV Wipe (dishppvwiipe.zip)
- 12 25.EDump (edump.zip)
- 13 26.Dish Hardware FAQ (faqdishhdwr.zip)
- 14 27.MCG305 (mcg305.zip)
- 15 28.E3m code (wese3mv3.zip)
- 16 29.Talk 3.1 (talk31.zip)

17 On or about June 24, 2001, a post to the Internet by "SatMedic" on
18 www.innermatrix.net "Satellite Chat" regarding "A note from DR7" in which he
19 posts the following authored by "DR7" [Menard] "*I have been here since day one
20 and ran the site [www.dr7.com] for almost 6 years now, 4 of those years I paid for
21 it out of my pockets with 0 advertisers and being one of the largest sites there was. I
22 lost my first real love who I had been with 5 years because I was addicted to this
23 fucking computer shit, I am now facing multimillion dollar lawsuits and the site is
24 done...so sad.*"

25 253. On or about December 16, 2001, Tarnovsky admits to Giles Kaehlin,
26 Head of Security for Canal+, at a meeting in London that NDS was responsible for
27 the hack and publication of the DISH Network ROM Code on the internet.
28 Tarnovsky admits that the DISH Network code was sent to him by Reuven Hasak,
head of security for NDS in Israel, from John Norris, head of security for NDS
Americas. Tarnovsky later sent an email stating that he [Tarnovsky] wanted no
further communications to occur between Tarnovsky and Kaehlin.

1 254. On or about January 9, 2002, *Norris purchased a “Karl Suss Probe”*
2 *manufactured by K&S, model 4524, serial number 610009, with a manual, for the*
3 *amount of \$18,500 for Tarnovsky. On or about January 17, 2002, the item was*
4 *shipped via Atlas Van Lines to “Chris Tarnovsky at 2339 Carioca Place, Vista,*
5 *California USA 92084, phone number 760-940-6147, fax number 760-940-6347.”*
6 *The invoice lists the “End User” to be Chris Tarnovsky at the same address.*

7 255. On or about August 30, 2002, *Norris purchased a “Karl Suss Probe (2*
8 *units), \$1,700” and had them sent to Chris Tarnovsky. One item, manufactured by*
9 *Karl Suss, was a model Probe for the amount of \$850. The other item was also*
10 *manufactured by Karl Suss and is a model Probe for the amount of \$850. On*
11 *August 30, 2002, the items were shipped via Federal Express to “Chris Tarnovsky*
12 *at 2339 Carioca Place, Vista, CA USA 92084, phone number 760-940-6147, and*
13 *fax number 760-940-6347.” The invoice lists the “End User” to be Chris*
14 *Tarnovsky.*

15 **b. Law Enforcement’s Investigation of Christopher**
16 **Tarnovsky, NDS Employee and Hacker for Satellite**
17 **Piracy**

18 256. On or about July 29, 2000, *“Chris Tarnovsky” of “737 Poppy Rd, San*
19 *Marcos, CA 92078, phone number 760-510-9487, DL # B9008318”, signed a*
20 *“Mailbox Rental Agreement” with “Mail and More, 925 E Hwy 80 PMB #245, San*
21 *Marcos, TX 78666.” Tarnovsky agreed to pay a \$7.00 per month rate for box #245,*
22 *for a total of \$84.00 for one year. He wrote into the agreement the following*
23 *instructions: “Forward all mail as arriving next day including Saturday. For voice*
24 *verification, ask dog name: answer “Princess.” For payment, Tarnovsky used*
25 *credit card number “4225-8106-5036-3909, expiration 12-01.”*

26 257. Tarnovsky received the following packages on the following dates at
27 “Mail and More” at his post office box address noted above:

28

1. On or about August 2, 2000, "X-Factor, X-Factor Design [Allen Menard's company], # 108-280 Nelson St., Vancouver, BC Canada, phone number 604-408-7762, UPS account number 49W-W48" sent a package to "CT [Tarnovsky], 925 E. highway 80 PMB #245, San Marcos, Texas 78666 USA, phone number 716-259-1580." The item enclosed was described as a "Sony Play Station manufactured in Japan" with tracking number "W601 911 651 5." The "Declaration of Contents and Shipper's Letter of Instruction" states that "X-Factor, X-Factor Design" shipped the package and describe the items enclosed as "one (1) Sony Psx Z, manufactured in Japan, valuing \$900.00; one (1) Sony Controller, manufactured in Japan, valuing \$30.00, and three (3) Sony CDs, manufactured in Japan, valuing \$60.00." The remarks section of the declaration reads "Birthday Gift." Tarnovsky's birthday listed on his California driver's license is April 20, 1971.
2. On or about August 11, 2000, the "Declaration of Contents and Shipper's Letter of Instruction" states that "Hi-Fi Exchange, 1750 Davie St. Suite 201, Vancouver, BC VGG-3B7, phone number 808-6026," sent one package weighing 11 pounds to "CT [Chris Tarnovsky] Electronics, 925 E Hwy 80 PMB #245, San Marcos, TX 78666." The item enclosed is described as "one (1) Technics Cassette Deck, manufactured in Singapore valued at \$350.00."
3. On or about August 15, 2000, the "Declaration of Contents and Shipper's Letter of Instruction" states that "Regency Audio, 1750 Drive, V663B7, Canada, phone number 604-808-6061" sent one package weighing 10 pounds to "CT [Chris Tarnovsky] Electronics, 925 E Hwy 80 #245, San Marcos, TX 78666, phone number 512-897-1677." The item enclosed is described as "one (1) Graphic Equalizer, manufactured in the USA, valuing \$300.00."
4. On or about August 23, 2000, a "Declaration of Contents and Shipper's Letter of Instruction" states that "Regency Audio, 1750 Davie #201, Van BC V663B1", sent one package weighing 10 pounds to "Owner, CT [Tarnovsky] Electronics, 925E Hwy 80 #245, San Marcos, TX 78666, phone number 396-1247." The item sent is described as "one (1) Sony Minidisk, manufactured in the USA, valuing \$350.00." The shipment was charged a \$62.78 transportation charge.

- 1 5. On or about August 25, 2000, "Regency, Regency Audio, 1750 Davie
2 3201, Van, BC VGB3B7, phone number 807-2262, UPS account
3 number 638X87", sent one package, with a weight of 11 pounds to
4 "CT [Tarnovsky], 925 E. highway 80 Suite 245, San Marcos, Texas
5 78666 USA, phone number 512-369-29." The item is described as a
6 "compact disc player manufactured in the USA." The tracking number
7 on the package was "W619 045 603 0." The package was sent
8 "expedited" with the special instructions "Zone 351."
9 6. On or about August 28, 2000, "Regency, Regency Audio, 1750 Davie
10 3201, Van, BC VGB3B7, phone number 807-2262, UPS account
11 number 638X87", sent one package, with an actual weight of 9 pounds
12 to "CT [Tarnovsky] Electronics, 925 E. highway 80 Suite 245, San
13 Marcos, Texas 78666 USA, phone number 512-369-4242." The item
14 was described as a "DVD Player manufactured in the USA." The
15 tracking number on the package was "W619 045 602 1", and the
16 package was sent "expedited."
17 7. On or about August 28, 2000, a package was sent to "Von," [Tarnovsky]
18 from "8132 Washburn Ct, Luling, TX 78648, phone number 703-850-
19 2337", with FedEx letter to "Chris Tarnovsky, 925 E. Hwy 80 #245, San
20 Marcos, TX 78666, phone number 703-850-2337." The parcel was sent
21 FedEx Priority Overnight with the tracking number "8153 1564 6118."
22 The sender, "Von," has an account that will be billed to pay for the
23 shipment. The parcel was to be delivered by August 29, 2000.
24 8. On or about August 29, 2000 a package was sent to "Von" [Tarnovsky]
25 from Mail & More, 925 Highway 80, San Marcos, Texas 78666, phone
26 number 703-850-2337, with a FedEx Envelope/Letter to "Chris
27 Tarnovsky, 737 Poppy Rd., San Marcos, CA 92078." The parcel was sent
28 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."

258. On or about August 29, 2000, an investigation by Detectives 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 San Marcos, Texas, and then forwarded to San Marcos, California

1 at Christopher Tarnovsky's expense. The caller advised "*there was no reason for*
2 *the parcel to be mailed to San Marcos, TX before being mailed to San Marcos,*
3 *CA.*" The investigation revealed that the return address and phone number on this
4 parcel was invalid. The name for the return address was "*Von*" [Tarnovsky].

5 259. The investigation further revealed that Chris Tarnovsky was living at
6 737 Poppy Road, San Marcos, California 92078. On July 29, 2000, and that he
7 rented mailbox number 245 at "Mail and More, 925 E.HWY 80, San Marcos, Hays
8 County, Texas." *Tarnovsky instructed the store manager to forward all of his mail*
9 *as arriving next day including Saturday to 737 Poppy Road, San Marcos,*
10 *California 92078. The store manager had been forwarding parcels to Tarnovsky*
11 *approximately "every day or every other day."* Tarnovsky falsely told the store
12 manager of Mail and More that he was a student at Southwest Texas State
13 University and was returning home to San Marcos, CA. However, the investigation
14 revealed that there was no record of Tarnovsky ever attending Southwest Texas
15 State University or living in the San Marcos, TX area.

16 260. On or about August 30, 2000, the store manager notified Detectives
17 that he received another parcel to be forwarded to Tarnovsky. The parcel was in a
18 JVC compact disc box with a return address of "*Regency Audio, 1750 Davis #201,*
19 *Van BC VGG3B7*" and addressed to "*CT [Tarnovsky] Electronics, 925 W HWY*
20 *suite 245, San Marcos, TX.*" Canines gave a positive alert at the presence of the
21 odor of marijuana or other illegal drugs after smelling the parcel. A search warrant
22 was then executed and *\$20,100.00 in US currency was discovered inside a medium*
23 *brown envelope taped to the circuitry inside the JVC compact disc player.*

24 261. On or about August 31, 2000, the store manager again notified the
25 investigating detective that a parcel had arrived. The parcel was identical to the one
26 received the day before, except the box was from a "*Pioneer DVD.*" Canines again
27 gave a positive alert at the suspected parcel. A second search warrant was executed
28

1 and \$20,000.00 in US currency was found in a medium sized envelope taped to the
2 circuitry of the DVD player.

3 262. On or about September 18, 2000, a 2 pound parcel with the dimensions
4 26 x 6 x 6 was shipped "PRIORITY OVERNIGHT" to "Chris Tarnovsky, 925 3
5 Hwy 80 PMB 245, San Marcos, TX 78666." The tracking number on the parcel was
6 4796 4348 4020. The parcel was to be delivered by September 19, 2000. The tag
7 is identified by account # 100467461, REP 7952771,1,9664120 (1), cad # 0052421
8 18SEP00, and the letters "XENIRA." The tag also shows "Digi-Key Corp., 701
9 Brooks Ave. S., Thief River Falls, MN 56701, (218)681-6674" as labeled
10 "Shipping."

11 263. On or about September 19, 2000, it was discovered that Tarnovsky
12 placed approximately 80 phone calls to Israel [NDS] and 120 to Belgium.
13 Tarnovsky also traveled over seas twice every six months going to Brussels and
14 other European countries. Tarnovsky had received two parcels at his residence from
15 Minnesota and Virginia [Tarnovsky Sr.].

16 264. On or about December 14, 2000, U.S. Customs advised the Hays
17 County Narcotics Task Force that Tarnovsky worked for NDS in California and was
18 believed to be counterfeiting or pirating satellite T.V. access cards. U.S. Customs
19 was, and currently is, working with Direct TV's private security company who was,
20 and currently is, also investigating Tarnovsky. Plaintiffs are informed and believe
21 that U.S. Customs also investigated Tarnovsky on a case in the States of Oregon
22 and Washington.

23 265. On or about January 9, 2001, a "knock and talk" by U.S. customs
24 agents Flannigan and Spears, as well as Ruben Romero of Galaxy Latin America,
25 takes place at at Tarnovsky's house in California. During the walkthrough, Agent
26 Flannigan sees a card emulator [device used for satellite piracy] pushing out smart
27 cards.

28

1 266. On or about February 9, 2001, U.S. Customs agents perform a raid on
2 Tarnovsky's house.

3 267. On or about March 8, 2001, at a meeting with Menard in Canada with
4 Ereiser present, *Menard stated that "Tarnovsky would lose his job"* if Menard
5 provided any information as to how the initial hack of EchoStar's conditional
6 access system occurred. Tarnovsky was an employee and agent of NDS at this time.

7 **VII. PLAINTIFFS HAVE BEEN, AND CONTINUE TO BE,**
8 **SUBSTANTIALLY INJURED BY DEFENDANTS' ILLEGAL**
9 **CONDUCT**

10 **1. As a Direct Result of Defendants Posting Plaintiffs'**
11 **EEPROM Code to the Internet, Plaintiffs' have had to, For**
12 **the Very First Time, Employ a Smart Card Swap of**
13 **Approximately More than 7 Million Smart Cards**

14 268. Since NDS's hacking the EchoStar/NagraStar smart card and posting
15 its EEPROM and ROM Codes on the Internet, Pirated EchoStar Access Cards and
16 other circumvention or signal theft devices designed to enable users to illegally
17 modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
18 (including, but not limited to, loaders, dead processor boot boards, glitches,
19 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
20 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
21 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
22 unlawful and unauthorized modification of and/or access to EchoStar's digital
23 satellite system) have become available.

24 269. These Pirated EchoStar Access Cards and other circumvention or
25 signal theft devices allow and facilitate the decryption of DISH Network's
26 Programming services without Plaintiffs' authorization or viewers' payment of the
27 necessary and required fees. These Pirated EchoStar Access Cards and other
28 circumvention or signal theft devices have been, and continue to be advertised and

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

8 270. Defendants' wrongful conduct has injured, and will continue to injure,
9 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
10 other valuable consideration, compromising Plaintiffs' security and accounting
11 systems, infringing Plaintiffs' trade secrets and proprietary information, and
12 interfering with Plaintiffs' contractual and prospective business relations.

13 **VI. CAUSES OF ACTION**

14 **FIRST CAUSE OF ACTION**

15 **(Circumventing Technological Measures Concerning Protected and** 16 **Copyrighted Works in Violation of the Digital Millennium Copyright Act, 17** 17 **U.S.C. § 1201(a)(1)(A))**

18 271. Plaintiffs re-allege and incorporate the above paragraphs as if fully set
19 forth in this cause of action.

20 272. Defendants circumvented Plaintiffs' technological measures contained
21 within EchoStar Access Cards which effectively control access to works protected
22 under Title 17 of the United States Code, namely DISH Network's satellite
23 television programming services and the protected works broadcasted thereon, by
24 altering, modifying, compromising, pirating, and/or reprogramming EchoStar
25 Access Cards to bypass EchoStar's encryption protection contained therein and to
26 enable the unauthorized access of copyrighted satellite television programming,
27 with each instance in violation of 17 U.S.C. § 1201(a)(1)(A).
28

1 273. These acts complained of herein occurred in, amongst other places, the
2 State of California, Canada, and Israel.

3 274. Defendants' acts of circumvention have been and continue to be
4 performed without the permission, authorization, or consent of Plaintiffs or any
5 owner of copyrighted programming broadcasted on the DISH Network.

6 275. Defendants have violated Section 1201(a)(1) of the DMCA willfully,
7 and for purposes of commercial advantage or private financial gain.

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

13 **SECOND CAUSE OF ACTION**

14 **(Manufacture of and Traffic in Signal Theft Devices in Violation of the Digital** 15 **Millennium Copyright Act, 17 U.S.C. § 1201(a)(2))**

16 277. Plaintiffs re-allege and incorporate the above as if fully set forth in this
17 cause of action.

18 278. Defendants were and are actively engaged in the business of
19 manufacturing, importing (to the United States), offering to the public, providing,
20 or otherwise trafficking in altered, modified, compromised, and/or counterfeit
21 EchoStar Access Cards ("Pirated EchoStar Access Cards") and other circumvention
22 or signal theft devices designed to enable users to illegally modify or alter EchoStar
23 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
24 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
25 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
26 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
27 other hardware and software intended for the unlawful and unauthorized
28 modification of and/or access to EchoStar's digital satellite system) knowing, or

1 having reason to know, that such Pirated EchoStar Access Cards and other
2 circumvention or signal theft devices designed to enable users to illegally modify or
3 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
4 limited to, loaders, dead processor boot boards, glitches, bootloaders, unloopers,
5 emulators, printed circuit boards, programmers, integrated receivers/decoders,
6 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
7 Locks, and/or other hardware and software intended for the unlawful and
8 unauthorized modification of and/or access to EchoStar's digital satellite system):
9 (a) are primarily designed or produced for the purpose of circumventing Plaintiffs'
10 encryption and conditional access technological measures that effectively control
11 access to copyrighted satellite television programming; (b) have only limited
12 commercially significant purpose or use other than to circumvent Plaintiffs'
13 encryption and conditional access technological measures that effectively controls
14 access to copyrighted programming; or (c) were marketed by Defendants, or others
15 acting in concert with Defendants with Defendants' knowledge, for use in
16 circumventing Plaintiffs' encryption and conditional access technological measures
17 Plaintiffs' encryption and conditional access technological measures that effectively
18 controls access to copyrighted programming, in violation of 17 U.S.C. § 1201(a)(2).

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

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

26 281. Defendants' acts of circumvention have been, and continue to be,
27 performed without the permission, authorization, or consent of Plaintiffs or any
28 owner of copyrighted programming.

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

4 283. Defendants knew, or should have known, that manufacturing,
5 importing (to the United States), offering to the public, providing, and trafficking in
6 Pirated EchoStar Access Cards and other circumvention or signal theft devices
7 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
8 Plaintiffs' Security System (including, but not limited to, loaders, dead processor
9 boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards,
10 programmers, integrated receivers/decoders, Audio Video Replicators "AVRs,"
11 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
12 software intended for the unlawful and unauthorized modification of and/or access
13 to EchoStar's digital satellite system) was and is illegal and prohibited.

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

18 **THIRD CAUSE OF ACTION**

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

21 285. Plaintiffs re-allege and incorporate the above as if fully set forth in this
22 cause of action.

23 286. Defendants were and are actively engaged in the business of
24 manufacturing, importing (to the United States), offering to the public, providing,
25 or otherwise trafficking in Pirated EchoStar Access Cards and other circumvention
26 or signal theft devices designed to enable users to illegally modify or alter EchoStar
27 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
28

1 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
2 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
3 Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and other
4 hardware and software intended for EchoStar’s digital satellite system) knowing, or
5 having reason to know, that such Pirated EchoStar Access Cards and other
6 circumvention or signal theft devices designed to enable users to illegally modify or
7 alter EchoStar Access Cards and/or Plaintiffs’ Security System (including, but not
8 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
9 emulators, printed circuit boards, programmers, integrated receivers/decoders,
10 Audio Video Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-
11 Locks, and/or other hardware and software intended for the unlawful and
12 unauthorized modification of and/or access to EchoStar’s digital satellite system):
13 (a) are primarily designed or produced for the purpose of circumventing the
14 protection afforded by Plaintiffs’ encryption and conditional access technological
15 measures that effectively protects rights of copyright owners in a work or portion
16 thereof; (b) have only limited commercially significant purpose or use other than to
17 circumvent the protection afforded by Plaintiffs’ encryption and conditional access
18 technological measures that effectively protects rights of copyright owners in a
19 work or portion thereof; or (c) were marketed by Defendants, or others acting in
20 concert with Defendants with Defendants’ knowledge, for use in circumventing
21 Plaintiffs’ encryption and conditional access technological measures Plaintiffs’
22 encryption and conditional access technological measures that effectively protects
23 rights of copyright owners in a work or portion thereof, in violation of 17 U.S.C. §
24 1201(b)(1).

25 287. These acts complained of herein occurred in, amongst other places, the
26 State of California, Canada, and Israel.

27 288. Defendants’ violations have injured, and will continue to injure,
28 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and

1 other valuable consideration, compromising Plaintiffs' security and accounting
2 systems, infringing Plaintiffs' trade secrets and proprietary information, and
3 interfering with Plaintiffs' contractual and prospective business relations.

4 289. Defendants' acts of circumvention have been, and continue to be,
5 performed without the permission, authorization, or consent of Plaintiffs or any
6 owner of copyrighted programming.

7 290. Defendants have violated Section 1201(b)(1) of the Digital
8 Millennium Copyright Act willfully, and for purposes of commercial advantage or
9 private financial gain.

10 291. Defendants knew, or should have known, that manufacturing,
11 importing (to the United States), offering to the public, providing, and trafficking in
12 Pirated EchoStar Access Cards and other circumvention or signal theft devices
13 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
14 Plaintiffs' Security System (including, but not limited to, loaders, dead processor
15 boot boards, glitches, bootloaders, unloopers, emulators, printed circuit boards,
16 programmers, integrated receivers/decoders, Audio Video Replicators "AVRs,"
17 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
18 software intended for the unlawful and unauthorized modification of and/or access
19 to EchoStar's digital satellite system) was and is illegal and prohibited.

20 292. Such violations have caused, and will continue to cause, Plaintiffs
21 irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such
22 continued violations. Unless restrained by this Court, Defendants will continue to
23 violate 17 U.S.C. § 1201(b)(1).

24 **FOURTH CAUSE OF ACTION**

25 **(Facilitating the Unauthorized Reception of Satellite Signals in Violation of the** 26 **Communications Act of 1934, as amended, 47 U.S.C. § 605(a))**

27 293. Plaintiffs re-allege and incorporate the above as if fully set forth in this
28 cause of action.

1 294. By designing, manufacturing, developing, manufacturing, assembling,
2 modifying, importing (to the United States), trafficking, distributing, and selling
3 Pirated EchoStar Access Cards and other circumvention or signal theft devices
4 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
5 Plaintiffs' Security System (including, but not limited to, loaders, dead processor
6 boot boards, glitches, bootloaders, unloopers, emulators, printed circuit boards,
7 programmers, integrated receivers/decoders, Audio Video Replicators "AVRs,"
8 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
9 software intended for the unlawful and unauthorized modification of and/or access
10 to EchoStar's digital satellite system), Defendants have assisted the unauthorized
11 reception of use of EchoStar's satellite transmissions of television programming by
12 persons not authorized to receive such transmissions, in violation of 47 U.S.C. §
13 605(a).

14 295. These acts complained of herein occurred in, amongst other places, the
15 State of California, Canada, and Israel.

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

21 297. Defendants' acts of circumvention have been, and continue to be,
22 performed without the permission, authorization, or consent of Plaintiffs or any
23 owner of copyrighted programming.

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

26 299. Defendants knew, or should have known, that assisting third person in
27 the reception and use of EchoStar's satellite transmissions of television
28 programming, without authorization, was and is illegal and prohibited.

1 300. 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.

5 301. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs are entitled to equitable
6 relief, damages (either statutory damages of \$1000 to \$10000 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 **FIFTH CAUSE OF ACTION**

11 **(Manufacture and Sale of Signal Theft Devices in Violation of the**
12 **Communications Act of 1934, as amended, 47 U.S.C. § 605(e)(4))**

13 302. Plaintiffs re-allege and incorporate the above as if fully set forth in this
14 cause of action.

15 303. Defendants have engaged in the business of manufacturing,
16 assembling, modifying, importing (to the United States), exporting, selling, and
17 distributing Pirated EchoStar Access Cards and other circumvention or signal theft
18 devices designed to enable users to illegally modify or alter EchoStar Access Cards
19 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
20 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
21 boards, programmers, integrated receivers/decoders, Audio Video Replicators
22 "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
23 and software intended for the unlawful and unauthorized modification of and/or
24 access to EchoStar's digital satellite system) knowing, or having reason to know,
25 that such Pirated EchoStar Access Cards and other circumvention or signal theft
26 devices designed to enable users to illegally modify or alter EchoStar Access Cards
27 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
28 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit

1 boards, programmers, integrated receivers/decoders, Audio Video Replicators
2 “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
3 and software intended for the unlawful and unauthorized modification of and/or
4 access to EchoStar’s digital satellite system) are primarily of assistance in the
5 unauthorized decryption of EchoStar’s satellite television programming services, or
6 are intended by Defendants to assist other persons in the unauthorized reception and
7 use of EchoStar’s satellite television programming services, in violation of 47
8 U.S.C. § 605(e)(4).

9 304. These acts complained of herein occurred in, amongst other places, the
10 State of California, Canada, and Israel.

11 305. Defendants’ acts of circumvention have been, and continue to be,
12 performed without the permission, authorization, or consent of Plaintiffs or any
13 owner of copyrighted programming.

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

19 307. Defendants have violated Section 605(e)(4) the Communications Act
20 willfully and for purposes of commercial advantage or private financial gain.

21 308. Defendants knew, or should have known, that manufacturing,
22 assembling, modifying, importing (to the United States), exporting, selling, and
23 distributing Pirated EchoStar Access Cards and other circumvention or signal theft
24 devices designed to enable users to illegally modify or alter EchoStar Access Cards
25 and/or Plaintiffs’ Security System (including, but not limited to, loaders, dead
26 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
27 boards, programmers, integrated receivers/decoders, Audio Video Replicators
28 “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware

1 and software intended for the unlawful and unauthorized modification of and/or
2 access to EchoStar's digital satellite system), primarily of assistance in the
3 unauthorized reception and decryption of EchoStar's satellite television
4 programming services, was and is illegal and prohibited.

5 309. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs are entitled to equitable
6 relief, damages (either statutory damages of \$1000 to \$10000 per violation, or
7 actual damages plus any profits realized by the Defendants and/or their agents as a
8 result of this unlawful conduct), and reasonable attorney's fees and costs. Plaintiffs
9 seek all other relief to which they may be entitled.

10 **SIXTH CAUSE OF ACTION**

11 **(Unauthorized Interception of Electronic Communications in Violation of the** 12 **Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)(a))**

13 310. Plaintiffs re-allege and incorporate the above as if fully set forth in this
14 cause of action.

15 311. By designing, developing, manufacturing, assembling, modifying,
16 importing (to the United States), exporting, trafficking, selling, and distributing
17 Pirated EchoStar Access Cards and other circumvention or signal theft devices
18 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
19 Plaintiffs' Security System (including, but not limited to, loaders, dead processor
20 boot boards, glitches, bootloaders, unloopers, emulators, printed circuit boards,
21 programmers, integrated receivers/decoders, Audio Video Replicators "AVRs,"
22 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
23 software intended for the unlawful and unauthorized modification of and/or access
24 to EchoStar's digital satellite system), and advertising and providing software,
25 information, and technical support services relating to Pirated EchoStar Access
26 Cards and other circumvention or signal theft devices designed to enable users to
27 illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
28 (including, but not limited to, loaders, dead processor boot boards, glitches,

1 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
2 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
3 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
4 unlawful and unauthorized modification of and/or access to EchoStar’s digital
5 satellite system), Defendants intentionally intercepted, endeavored to intercept, or
6 procured other persons to intercept or endeavor to intercept, EchoStar’s satellite
7 transmissions of television programming, in violation of 18 U.S.C. § 2511(1)(a).

8 312. These acts complained of herein occurred in, amongst other places, the
9 State of California, Canada, and Israel.

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

15 314. Defendants have engaged in conduct in violation of Section 2511(1)(a)
16 of the Electronic Communications Privacy Act for a tortious or illegal purpose, or
17 for purposes of direct or indirect commercial advantage or private commercial gain.

18 315. Defendants knew, or should have known, that such interception of
19 EchoStar’s satellite transmissions of television programming was and is illegal and
20 prohibited.

21 316. Such violations have caused and will continue to cause Plaintiffs
22 irreparable harm and Plaintiffs have no adequate remedy at law to redress any such
23 continued violations. Unless restrained by this Court, Defendants will continue to
24 violate 18 U.S.C. § 2511(1)(a).

25 SEVENTH CAUSE OF ACTION

26 **(Trademark Infringement in Violation of the Lanham Act, 15 U.S.C. § 1114)**

27 317. Plaintiffs re-allege and incorporate the above as if fully set forth in this
28 cause of action.

1 318. EchoStar has adopted the mark “DISH Network“ and used it in
2 interstate commerce for equipment, goods, and services sold or licensed by
3 EchoStar as part of its direct broadcast satellite system. On February 5, 1995, an
4 application for registration of said mark was filed in the United States Patent and
5 Trademark Office. On May 5, 1998, said mark was registered in the United States
6 Patent and Trademark Office on the Principal Register under the Act of 1946
7 covering the use of said mark on equipment, goods, and services sold or licensed by
8 EchoStar as part of its direct broadcast system. EchoStar’s registration is now
9 outstanding and valid.

10 319. Defendants have infringed EchoStar’s mark in interstate and foreign
11 commerce by various acts including, but not limited to, designing, manufacturing,
12 importing, distributing, selling, offering for sale, and advertising Pirated EchoStar
13 Access Cards and other circumvention or signal theft devices designed to enable
14 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs’ Security
15 System (including, but not limited to, loaders, dead processor boot boards,
16 glitches, bootloaders, unloopers, emulators, printed circuit boards, programmers,
17 integrated receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers,
18 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
19 for the unlawful and unauthorized modification of and/or access to EchoStar’s
20 digital satellite system under the name and mark of “DISH Network.” Defendants’
21 use of EchoStar’s mark is without permission or authority of EchoStar and said use
22 is likely to cause confusion, mistake, and deceit.

23 320. These acts complained of herein occurred in, amongst other places, the
24 State of California, Canada, and Israel.

25 321. Defendants, individually and as members of the conspiracy, have
26 engaged in conduct in violation of 15 U.S.C. § 1114 with the intent to cause
27 confusion, mistake, and deceit.

28

1 322. Defendants knew, or should have known, that their use of the “DISH
2 Network” mark (1) on Pirated EchoStar Access Cards that Defendants designed,
3 manufactured, imported (to the United States), distributed, and sold, (2) on other
4 circumvention or signal theft devices designed to enable users to illegally modify or
5 alter EchoStar Access Cards and/or Plaintiffs’ Security System (including, but not
6 limited to, loaders, dead processor boot boards, glitches, bootloaders, unloopers,
7 emulators, printed circuit boards, programmers, integrated receivers/decoders,
8 Audio Video Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-
9 Locks, and/or other hardware and software intended for the unlawful and
10 unauthorized modification of and/or access to EchoStar’s digital satellite system)
11 that Defendants designed, manufactured, imported (to the United States),
12 distributed, and sold, and (3) on Defendants’ advertisements for the sale and use of
13 Pirated EchoStar Access Cards and other circumvention or signal theft devices
14 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
15 Plaintiffs’ Security System (including, but not limited to, loaders, dead processor
16 boot boards, glitches, bootloaders, unloopers, emulators, printed circuit boards,
17 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”
18 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
19 software intended for the unlawful and unauthorized modification of and/or access
20 to EchoStar’s digital satellite system) was and is illegal and prohibited. Such
21 violations have caused and will continue to cause Plaintiffs irreparable harm, and
22 Plaintiffs have no adequate remedy at law to redress any such continued violations.
23 Unless restrained by this Court, Defendants will continue to violate 15 U.S.C. §
24 1114.

25 **EIGHTH CAUSE OF ACTION**
26 **(Use of False Designation in Violation of the Lanham Act,**
27 **15 U.S.C. § 1125(a))**
28

1 323. Plaintiffs re-allege and incorporate the above as if fully set forth in this
2 cause of action.

3 324. Defendants have caused Pirated EchoStar Access Cards and other
4 circumvention or signal theft devices designed to enable users to illegally modify or
5 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
6 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
7 emulators, printed circuit boards, programmers, integrated receivers/decoders,
8 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
9 Locks, and/or other hardware and software intended for the unlawful and
10 unauthorized modification of and/or access to EchoStar's digital satellite system) to
11 enter into interstate and foreign commerce with the designation and representation
12 "DISH Network" connected therewith. Defendants' use of "DISH Network" is a
13 false designation of origin which is likely to cause confusion, mistake, and deceit as
14 to the affiliation, connection, or association of Defendants with EchoStar and as to
15 the origin, sponsorship, or approval of such goods and services by EchoStar.

16 325. These acts complained of herein occurred in, amongst other places, the
17 State of California, Canada, and Israel.

18 326. Defendants' actions are in violation of 15 U.S.C. § 1125(a) in that
19 Defendants have used in connection with goods and services advertised and sold by
20 Defendants a false designation of origin, a false or misleading description and
21 representation of fact which is likely to cause confusion, mistake, and deceit as to
22 the affiliation, connection, or association of Defendants with EchoStar and as to the
23 origin, sponsorship, or approval of Defendants' goods, services, and commercial
24 activities by EchoStar.

25 327. Defendants, individually and as members of the conspiracy, have
26 engaged in conduct in violation of 15 U.S.C. § 1125(a) with the intent to cause
27 confusion, mistake, and deceit.

28

1 328. Defendants knew, or should have known, that their false designation of
2 origin and their false or misleading description and representation of fact were and
3 are illegal and prohibited. Such violations have caused and will continue to cause
4 Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress
5 any such continued violations. Unless restrained by this Court, Defendants will
6 continue to violate 15 U.S.C. § 1125(a).

7 **NINETH CAUSE OF ACTION**

8 **(RICO, 18 U.S.C. § 1962(c))**

9 329. Plaintiffs re-allege and incorporate the above as if fully set forth in this
10 cause of action.

11 330. Defendants' unlawful, tortious and otherwise actionable conduct as
12 alleged in Plaintiffs' SAC constitutes a pattern of of "racketeering activity" as
13 defined by 18 U.S.C. § 1961.

14 331. Defendants committed at least the following predicate acts: (i) criminal
15 copyright infringement in violation of 17 U.S.C. § 506(a) and 18 U.S.C. § 2319; (ii)
16 misconduct in connection with access devices in violation of 18 U.S.C. § 1029; and
17 (iii) wire fraud in violation of 18 U.S.C. § 1343. Defendants produced, trafficked
18 in, controlled, and possessed device making equipment in violation of 18 U.S.C. §
19 1029(a)(4).

20 332. Each of these violations by Defendants Norris, Hasak, Tarnovsky,
21 Kommerling, Luyando, among others, of 18 U.S.C. §§ 1029, 1341, 1343, and 2319,
22 constitutes an instance of "racketeering activity" as defined in 18 U.S.C. § 1961(1),
23 and was committed in furtherance of the conspiracy to compromise and make
24 available EchoStar's proprietary information to the general public for an illegal use.
25 Defendants Norris, Hasak, Tarnovsky, Kommerling, Luyando, among others, and
26 each of them, aided and abetted the commission of these violations of 18 U.S.C. §§
27 1029, 1341, 1343, and 2319.

28

1 333. At all times relevant, Defendants NDS, Norris, Hasak, Kommerling,
2 Luyando, Tarnovsky, Menard, and Menard's distribution network consisting of
3 Defendants Quinn, Sergei, Dawson, and Frost, among others, ("distribution
4 network") were associated-in-fact through their continuing efforts from as early as
5 1998 to present to compromise, and make available to the general public for
6 improper and illegal use, EchoStar's proprietary information including, but not
7 limited to, EchoStar's secret ROM and EEPROM Codes, Pirated EchoStar Access
8 Cards and other circumvention or signal theft devices designed to enable users to
9 modify or alter EchoStar Access cards to receive and view EchoStar Programming
10 without authorization, and software programs, technical support services, and fixes
11 designed and intended to circumvent Plaintiffs' ECMs that instituted primarily to
12 disable Defendants' illegal devices and/or support services. Such association in
13 fact constitutes an enterprise as defined in 18 U.S.C. §1961(4).

14 334. Defendant NDS specifically functioned to oversee and coordinate the
15 implementation of specific acts by the various Defendants including, but not limited
16 to, Defendants Norris, Hasak, Kommerling, Luyando, Tarnovsky, Menard, and
17 Menard's distribution network, made strategic decisions concerning the extraction
18 of Plaintiffs' secret ROM and EEPROM Codes, the design and manufacture of
19 Pirated EchoStar Access Cards and other circumvention or signal theft devices
20 designed to enable users to modify or alter EchoStar Access cards to receive and
21 view EchoStar Programming without authorization, and facilitated communication
22 between the various Defendants referenced herein. Specifically, Defendant NDS
23 directed the affairs of Defendants Norris, Hasak, Kommerling, Luyando,
24 Tarnovsky, Menard, and Menard's distribution network on an ongoing basis and
25 recruited and attempted to recruit others for the enterprise including, but not limited
26 to, Norm Dick and John Greyson. Defendant NDS also made decisions about the
27 information that was to be made available to the general public in addition to
28 manner and timing of the release of Plaintiffs' secret ROM and EEPROM Codes,

1 select portions thereof, and/or specific and detailed instructions on how to extract
2 same, the design and manufacture of Pirated EchoStar Access Cards and other
3 circumvention or signal theft devices designed to enable users to modify or alter
4 EchoStar Access cards to receive and view EchoStar Programming without
5 authorization. This constitutes an organization separate and apart from the activity
6 in which NDS was engaged.

7 335. Defendants and/or their agents have an organizational structure or
8 system of authority for making and implementing decisions and for exercising
9 common control over its members.

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

23 337. Menard is or was the primary decisionmaker of the distribution and
24 sale structure of the enterprise, controlling and directing the affairs of the group on
25 an ongoing basis and recruiting the various individual Defendants and/or their
26 agents. Menard exerted control over the direction of the enterprise by, for example,
27 selling devices that allowed the pirates to operate as "dealers" of altered Access
28 Cards. Those associated with Defendants constituted a distribution network for the

1 altered Access Cards and pirate technology. They imported, exported, concealed,
2 and sold altered Access Cards to subscribers and prospective subscribers
3 throughout the United States and elsewhere. They used pirate technology,
4 including programmers, to manufacture and repair altered Access Cards. These
5 actions were taken in furtherance of the enterprise's goal of harming Plaintiffs and
6 decreasing Plaintiffs' competitiveness.

7 338. NDS is or was the primary decisionmaker of the technology structure
8 of the enterprise, controlling and directing the affairs of Christopher Tarnovsky on
9 an ongoing basis and recruiting or attempting to recruit others for the enterprise.
10 NDS exerted control over the direction of the enterprise by, for example, employing
11 or attempting to employ individuals to hack or break the Security System, and by
12 determining what technology and information would be made available to harm
13 Plaintiffs. The enterprise is more than the sum of its racketeering activity.

14 339. The distribution side, and the technology side, of the organization and
15 structure discussed herein functioned as a continuing unit and were controlled
16 primarily by the single-decision making apparatus within NDS, which determined
17 when and what hacked software code to release to the public.

18 340. The central decision making apparatus within NDS's was able to
19 control Menard and his distribution network by, *inter alia*, (a) NDS bestowed upon
20 Menard the ability to reprogram EchoStar smart cards by providing Menard with a
21 sophisticated reprogrammer device (coined by Tarnovsky as "the stinger") designed
22 and built by NDS and Tarnovsky using the proprietary information NDS unlawfully
23 obtained from the microprocessor embedded in Plaintiffs' smart cards at the NDS
24 laboratory in Haifa, Israel; (b) controlling the number of EchoStar smart cards that
25 Menard was able to unlawfully reprogram, and ultimately distribute to pirating end-
26 users via his distribution network, by instructing and/or assisting Tarnovsky in
27 writing software codes that operated the NDS/Tarnovsky reprogrammer in a
28 "CONTROLLED" manner such that it would automatically become disabled after

1 reprogramming a predetermined number of Plaintiffs' smart cards; (c) controlling
2 Menard's ability to 'reactivate' the NDS/Tarnovsky reprogrammer – to wit,
3 Tarnovsky would not send software and/or command codes to reactivate the
4 reprogramming device until instructed to do so by NDS; (d) controlling which
5 specific portions of Plaintiffs' proprietary code that Menard could publically post
6 on his www.dr7.com website as well as when such posts could be effectuated; (e)
7 controlling the specific type, generation or version of Plaintiffs' smart cards that
8 Menard was able to reprogram and ultimately provide to the pirating end-users via
9 his distribution network; (f) controlling if, when, how and where the unlawfully
10 reprogrammed EchoStar smart cards distributed by Menard and his distribution
11 network would be reactivated and/or repaired after Plaintiffs launched an electronic
12 counter measure to disable these cards by deciding whether to provide Menard a
13 "fix", "update" or "counter ecm", among other technical support, in which to post
14 on his website or wether to have Tarnovsky physically write a new code to repair
15 said cards in which case Menard and his distribution network would be required to
16 re-acquire these distributed cards and load them back into the NDS/Tarnovsky
17 reprogrammer; (g) controlling the price (and conversely, the supply and demand
18 market) that Menard and his distribution network were able to distribute these
19 pirated EchoStar smart cards for; (h) controlling the degree of protection NDS
20 would provide and when such protection was provided to Menard and the members
21 of his distribution network by, *inter alia*, running interference with and/or
22 providing information to the Canadian RCMP; and (i) controlling when and how
23 NDS/Tarnovsky would effectuate the wide spread compromise of Plaintiffs
24 conditional access system – which ultimately occurred via Tarnovsky's December
25 23 and 24, 2000 posts on Menard's website, among others.

26 341. Defendants knowingly produced, trafficked in, controlled, and
27 possessed "device making equipment" – any equipment, mechanism, or impression
28

1 designed or primarily used for making an access device or counterfeit access device
2 – in violation of 18 U.S.C. § 1029, by at least the following:

- 3 - On or about April 5, 1999, a post to the Internet by “DR7” [Menard] states
4 that Menard “visited Discount [Discount Satellite/Dawson] this aft, got card
5 reloaded with bootstrap and main.enc file and some other small one that
6 some program made, bat card now fully functioning.”
- 7 - On or about April 20, 1999, Dawson and Discount Satellite were raided in
8 Edmonton by the RCMP; local reports regarding Dawson’s selling
9 pirated EchoStar access cards and other illegal signal theft devices on his
10 Internet website, www.discountsatellite.com. Among the items confiscated
11 were illegal satellite access cards, computers, and other equipment used to
12 program access cards, approximately \$69,500 in U.S. and Canadian money
13 orders and cash, and drugs. Dawson continued to operate his illegal business
14 in Canada through his website, www.discountsatellite.com.
- 15 - On or about October 6, 1999, a post to the Internet by “Code” [Tarnovsky],
16 concerning a new circumvention or signal theft device called an AVR, states
17 “if the key servers are working correctly, you will know the new avr key
18 they [DISH Network] are about to switch to in advance!”
- 19 - On or about October 6, 1999, a post to the Internet by “JD” [Dawson],
20 concerning inquiry to purchase AVR devices, states “we [Defendants] have
21 available to us now an aftermarket avr device that will activate all channels
22 on the Echostar Dishnetwork system. It runs without the use of the original
23 plastic card and is totally supported via the internet. It is NOT an auto-
24 update product and will stop working in the event of a keychange.
25 HOWEVER, key updates are posted within minutes and available to all. . . .
26 Total cost for board and programmer is currently 150.00 usd. Or 110.00 usd
27 for just the avr board.”
- 28 - On or about September 8, 2000, a post to the Internet by “DR7” [Menard]
stating “I have only honestly patched 3 times in 18 months...where do they
get the info they post about E3m [the EchoStar hack by NDS, its agents
Tarnvosky, Menard and others] being so bad??...I have had one [ECM] since
day one when discount [Discount 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.”

- 1 - On or about November 21, 2000, a post to the Internet by "Koinvizion"
2 [Sergei] announcing that [Defendants] can now fix the "smartcard not
3 inserted correctly Error for \$50.00USD per card + the usual shipping charges
4 for everyone."
5 - On or about December 29, 2000, a post to the Internet by "hitek" [Sean
6 Quinn], entitled "e3m cards," states "the new group wants to sell the
7 machines now...please e-mail us and we will give you info on the machines
8 as well as where you can order it from...30 machines ready to go."

9 342. Defendants engaged in mail fraud in violation of 18 U.S.C. § 1341
10 when Defendants transmitted, by means of United States Postal Service and/or
11 commercial interstate and foreign carriers, at least the following:

- 12 - On or about April 16, 1999, NDS letter was sent from Adams to Hasak
13 concerning, among other things, a piracy investigation of www.dr7.com and
14 "DR7" [Al Menard]. Adams states, "[s]omewhere in the loop appears
15 PINKERTON investigative Service. They at one time worked for Irdeto as
16 well as other companies. There is talk that an agency is investigating
17 DR7[Menard]."
18 - On or about June 18, 1999, a NDS Letter to Hasak from Adams concerning
19 NDS's hiring satellite pirates and hackers in order to "CONTROL" them as
20 well as NDS's fear of losing its contract with DirecTV to be DirecTV's smart
21 card provider.
22 - On or about August 2, 2000, "X-Factor, X-Factor Design [Menard's
23 company], # 108-280 Nelson St., Vancouver, BC Canada, phone number
24 604-408-7762, UPS account number 49W-W48" sent a package to "CT
25 [Tarnovsky], 925 E. highway 80 PMB #245, San Marcos, Texas 78666 USA,
26 phone number 716-259-1580." The item enclosed was described as a "Sony
27 Play Station manufactured in Japan" with tracking number "W601 911 651
28 5." Menard sent the "expedited" with the special instructions "UPS CALL
MBE 1ST ON ANY SHIPPER ISSUE." The "Declaration of Contents and
Shipper's Letter of Instruction" states that "X-Factor, X-Factor Design"
shipped the package and describe the items enclosed as "one (1) Sony Pxs Z,
manufactured in Japan, valuing \$900.00; one (1) Sony Controller,
manufactured in Japan, valuing \$30.00, and three (3) Sony CDs,
manufactured in Japan, valuing \$60.00." The remarks section of the

1 declaration reads "Birthday Gift." Tarnovsky's birthday listed on his
2 California driver's license is April 20, 1971.

- 3 - On or about August 11, 2000, a "Declaration of Contents and Shipper's
4 Letter of Instruction" states that "Hi-Fi Exchange, 1750 Davie St. Suite 201,
5 Vancouver, BC VGG-3B7, phone number 808-6026," sent one package
6 weighing 11 pounds to "CT Electronics, 925 E Hwy 80 PMB #245, San
7 Marcos, TX 78666." The item enclosed is described as "one (1) Technics
8 Cassette Deck, manufactured in Singapore valued at \$350.00."
9
10 - On or about August 15, 2000, a "Declaration of Contents and Shipper's
11 Letter of Instruction" states that "Regency Audio, 1750 Drive, V663B7,
12 Canada, phone number 604-808-6061" sent one package weighing 10 pounds
13 to "CT [Chris Tarnovsky] Electronics, 925 E Hwy 80 #245, San Marcos, TX
14 78666, phone number 512-897-1677." The item enclosed is described as
15 "one (1) Graphic Equalizer, manufactured in the USA, valuing \$300.00."
16
17 - On or about August 23, 2000, a "Declaration of Contents and Shipper's
18 Letter of Instruction" states that "Regency Audio, 1750 Davie #201, Van BC
19 V663B1", sent one package weighing 10 pounds to "Owner, CT [Tarnovsky]
20 Electronics, 925E Hwy 80 #245, San Marcos, TX 78666, phone number 396-
21 1247." The item sent is described as "one (1) Sony Minidisk, manufactured
22 in the USA, valuing \$350.00." The shipment was charged a \$62.78
23 transportation charge.
24
25 - On or about August 25, 2000, "Regency, Regency Audio, 1750 Davie 3201,
26 Van, BC VGB3B7, phone number 807-2262, UPS account number 638X87",
27 sent one package, with a weight of 11 pounds to "CT [Tarnovsky], 925 E.
28 highway 80 Suite 245, San Marcos, Texas 78666 USA, phone number 512-
369-29." The item is described as a "compact disc player manufactured in
the USA." The tracking number on the package was "W619 045 603 0."
The package was sent "expedited" with the special instructions "Zone 351."
- On or about August 28, 2000, "Regency, Regency Audio, 1750 Davie 3201,
Van, BC VGB3B7, phone number 807-2262, UPS account number 638X87",
sent one package, with an actual weight of 9 pounds to "CT [Tarnovsky]
Electronics, 925 E. highway 80 Suite 245, San Marcos, Texas 78666 USA,
phone number 512-369-4242." The item was described as a "DVD Player
manufactured in the USA." The tracking number on the package was "W619
045 602 1", and the package was sent "expedited."

- 1 - On or about August 28, 2000, a package was sent to "Von," [Tarnovsky]
2 from "8132 Washburn Ct, Luling, TX 78648, phone number 703-850-2337",
3 with FedEx letter to "Chris Tarnovsky, 925 E. Hwy 80 #245, San Marcos,
4 TX 78666, phone number 703-850-2337." The parcel was sent FedEx
5 Priority Overnight with the tracking number "8153 1564 6118." The sender,
6 "Von," has an account that will be billed to pay for the shipment. The parcel
7 was to be delivered by August 29, 2000.
- 8 - On or about August 29, 2000 a package was sent to "Von" [Tarnovsky] from
9 Mail & More, 925 Highway 80, San Marcos, Texas 78666, phone number
10 703-850-2337, with a FedEx Envelope/Letter to "Chris Tarnovsky, 737
11 Poppy Rd., San Marcos, CA 92078." The parcel was sent FedEx Priority
12 Overnight with the tracking number "8213 3536 0680." Tarnovsky, "Von,"
13 has an account, number "1700-1825-7" that is billed for the shipment. The
14 FedEx tag is marked "XENIRA."
- 15 - On or about August 29, 2000, an investigation by a Detective at the Hays
16 County Narcotics Task Force was conducted in response to an anonymous
17 call from a concerned citizen stating that a suspicious parcel had been mailed
18 from Luling, Texas to San Marcos, Texas, and then forwarded to San
19 Marcos, California at Tarnovsky's expense. The caller advised "there was no
20 reason for the parcel to be mailed to San Marcos, TX before being mailed to
21 San Marcos, CA." The investigation revealed that the return address and
22 phone number on this parcel was invalid. The name for the return address
23 was "Von" [Tarnovsky]. he investigation further revealed that Chris
24 Tarnovsky was living at 737 Poppy Road, San Marcos, California 92078. On
25 July 29, 2000, he rented mailbox number 245 at "Mail and More, 925
26 E.HWY 80, San Marcos, Hays County, Texas." In doing so, Tarnovsky
27 falsely told the store manager that he was a student at Southwest Texas State
28 University and was returning home to San Marcos, CA. However, there was
no record of Tarnovsky ever attending Southwest Texas State University or
living in the San Marcos, TX area. Tarnovsky instructed the store manager
to forward all of his mail as arriving next day including Saturday to 737
Poppy Road, San Marcos, California 92078. The store manager had been
forwarding parcels to Tarnovsky approximately "every day or every other
day."
- On or about August 30, 2000, the store manager notified the investigating
detective that he received another parcel to be forwarded to Tarnovsky. The
parcel was in a JVC compact disc box with a return address of "Regency
Audio, 1750 Davis #201, Van BC VGG3B7" and addressed to "CT

1 [Tarnovsky] Electronics, 925 W HWY suite 245, San Marcos, TX.” Canines
2 gave a positive alert at the presence of the odor of marijuana or other illegal
3 drugs after smelling the parcel. A search warrant was then executed and
4 \$20,100.00 in US currency was discovered inside a medium brown envelope
taped to the circuitry inside the JVC compact disc player.

- 5 - On or about August 31, 2000, the store manager again notified the
6 investigating detective that a parcel had arrived. The parcel was identical to
7 the one received the day before, except the box was from a “Pioneer DVD.”
8 Canines again gave a positive alert at the suspected parcel. A second search
9 warrant was executed and \$20,000.00 in US currency was found in a medium
10 sized envelope taped to the circuitry of the DVD player.
- 11 - On or about November 21, 2000, a post to the Internet by “Koinvizion”
12 [Sergei] announcing that [Defendants] can now fix the “smartcard not
13 inserted correctly Error for \$50.00USD per card + the usual shipping charges
14 for everyone.”
- 15 - On or about December 1, 2000, a post to the Internet by “Kingtut” stating “I
16 just got my cards from koin [Andre Sergi].”
- 17 - On or about January 9, 2002, Norris purchased a “Karl Suss Probe”
18 manufactured by K&S, model 4524, serial number 610009, with a manual,
19 for the amount of \$18,500 for Tarnovsky. On or about January 17, 2002, the
20 item was shipped via Atlas Van Lines to “Chris Tarnovsky at 2339 Carioca
21 Place, Vista, California USA 92084, phone number 760-940-6147, fax
22 number 760-940-6347.” The invoice lists the “End User” to be Chris
23 Tarnovsky at the same address.
- 24 - On or about July 26, 2002, Tarnovsky purchased a manufactured “Karl Suss,
25 model PM-8” for the amount of \$15,000. On or about August 15, 2002, the
26 item was shipped via Federal Express to Chris Tarnovsky at 2339 Carioca
27 Place, Vista, California USA 92084, phone number 760-940-6147, fax
28 number 760-940-6347. The invoice lists the “End User” to be Chris
Tarnovsky.
- On or about August 30, 2002, Norris purchased a “Karl Suss Probe (2 units),
\$1,700” and had them sent to Tarnovsky. One item, manufactured by Karl
Suss, was a model Probe for the amount of \$850. The other item was also
manufactured by Karl Suss and is a model Probe for the amount of \$850. On
August 30, 2002, the items were shipped via Federal Express to “Chris
Tarnovsky at 2339 Carioca Place, Vista, CA USA 92084, phone number 760-

1 940-6147, and fax number 760-940-6347.” The invoice lists the “End User”
2 to be Chris Tarnovsky.

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

- 6
- 7 - On or about November 20, 1998, a post to the Internet by “DR7” [Menard],
8 concerning the EchoStar hack, states: “a file was sent too me recently by
9 Swiss cheese boys [Tarnovsky] and they asked me too add, lins too it are in
10 todays news 11.20.98 and it is also added to the Echostar tools section, sorry
11 I didn’t have more info with this text file but I think a few of you could use
12 this info...thanks again too the Users of this forum who have contributed
13 their time to the Echostar Project as well as the SCP [Tarnovsky] for
14 initiating this...good luck guys and hope to have more info shortly.”
 - 15 - On or about December 4, 1998, a post to the Internet by “Nipper”
16 [Tarnovsky] providing Plaintiffs’ Bat keys.
 - 17 - On or about December 7-8, 1998, a post to the Internet by “Nipper”
18 [Tarnovsky] supplying illegally obtained information concerning DISH
19 Network.
 - 20 - On or about March 26, 1999, a post to the Internet by “DR7” [Menard]
21 states: “the CAM dump is posted in the Tools section... Echostar Running
22 Card Dump + Public Keys by Swiss Cheese Productions [Tarnovsky]”
 - 23 - In or around April 1999, Menard telephoned Scullion again to solicit
24 Scullion’s participation in a distribution network to sell Pirated EchoStar
25 Access Cards. During this conversation, Menard informed Scullion that he
26 was close to receiving a full hack of the EchoStar system and that, “due to
27 the pirate community’s interest in Swiss Cheese Production’s stuff,” the plan
28 was a guaranteed money maker. Menard also informed Scullion that the
distribution network was going to have something special attached with its
operation: protection of NDS. Menard informed Scullion that “NDS was the
entity whom had ordered the hack and the distribution of pirated cards
through Menard’s distribution network.” Menard also informed Scullion
that “NDS had an arrangement with Tarnovsky to provide the support and
facilitation of the hacked EchoStar code to be sent to Menard to be used in
the distribution network.” Menard also informed Scullion that Scullion had
nothing to worry about with respect to being raided by the RCMP due to the

1 fact that “NDS was connected and had a solid relationship [with the
2 RCMP].” Menard further informed Scullion that “NDS would be running
3 interference in the distribution network.”

- 4 - On or about April 10, 1999, a post to the Internet by “DR7” [Menard] where
5 he inserts a private chat he had with “CanBert” including “went to jd’s
6 [Discount Satellite/Dawson] today; if I send my batt [illegal battery card] in
7 how much to get it fixed??.; not sure...never heard the price when I was
8 there...customers pay \$40; you’ll have to call; at Discount Sat??.; yes 780-
9 448-1787; thankx DR7; np man.”
- 10 - May 9, 1999, a post to the Internet states that the “Echostar update for the
11 commercial battery cards has been released and is confirmed working again.
12 The file can be downloaded from [Dawson’s website]
13 www.discountsatellite.com/Efile.zip.”
- 14 - On or about May 19, 1999, a post to the Internet by “DR7” [Menard] states
15 that he asked JD [Dawson] why the bat [battery card] isn’t autorolling
16 [automatically finding keys to counter ECMS]. JD [Dawson] stated the
17 reason was the requirement to hand out a bootstrap and that the potential
18 source code would have to be released.
- 19 - In April 1999, Menard telephoned Reginald Scullion with an offer to
20 participate in the “DISH Network” hack. During these conversations, Menard
21 informed Scullion that, among other things: (a) NDS was behind the
22 EchoStar hack; (b) the Tarnovsky/Menard distribution model would be
23 protected and controlled by NDS; (c) NDS had an arrangement with
24 Tarnovsky to provide the technical and software support and facilitate the
25 hacked EchoStar ROM Code to be sent to Menard and used in the
26 distribution network; and (d) NDS would protect this distribution network
27 from potential RCMP raids.
- 28 - On or about July 6, 1999, a post to the Internet by “DR7” [Menard] states
that “marry3M is used for JD’s [Dawson’s] 3M customers to do the
following: Write IRD# Write Key# Read Key# from card with sub/previous
sub Set zipcode/timezone.”
- On or about August 10, 1999, a post to the Internet by “Nipper” [Tarnovsky]
providing EchoStar Bat keys.

- 1 - On or about August 21, 1999, a post to the Internet by "DR7" [Menard]
2 states that Menard called "JD" [Dawson] to confirm status of file and JD
3 [Dawson] stated that he would "post REV20A.E3M on his website."
- 4 - On or about September 8, 1999, a post to the Internet by "xbr21"
5 [Tarnovsky], quoting "Nipper's" [Tarnovsky's] previous post, stating "here
6 is a neat no-mod trick- send out a control work packet using a key offset of
7 07 (eg 05/15/07). Card should skip decript of packet and simply encrypt with
8 your boxkey!! Simple and why not use this on channel 101? Another
9 example of stupidity."
- 10 - On or about September 29, 1999, a post to the Internet by "DR7" [Menard]
11 states that he talked to "JD" [Dawson] on the phone about 20 minutes ago
12 and JD [Dawson] said that he would also just "sell the programmed [DISH
13 Network] chip" if there was a demand for it. A later post to the Internet, on
14 the same date, by "DR7" [Menard] stating that he "confirmed with JD
15 [Dawson] that the keys in the latest talk.cfg file are not for AVR freeware
16 and will only work on JD's [Dawson's] AVR."
- 17 - On or about October 19, 1999, a post to the Internet by "DR7" [Menard]
18 announced that "'xfile 2.01' and 'Blocker version 2.3 Beta' were posted to
19 the Echo files section of the DR7 website." "DR7" [Menard] further states
20 "sorry they were not posted earlier but the creators [Defendants/Tarnovsky]
21 never bothered to send them so basically I couldn't post what I didn't have,
22 thanks to those that did send them."
- 23 - In November 1999, Menard again telephoned Reginald Scullion with an offer
24 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
28 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.
- On or about November 9, 1999, a post to the Internet by "DR7" [Menard],
regarding "JD's [Dawson's] gone???", states "since Friday I have not been
able at all to call your shop and get through, I tried over 20 times per day at
least just to test. JD [Dawson] this is getting outta hand and now its come to
the point where I am looking bad for advertising for you and also for being in
same city, I think you owe these people an explanation as well as an apology

1 and shouldn't expect me to have to deal with any of this...I am now removing
2 Discount Satellite advertising banners from this website JD [Dawson]
3 because I cannot and will not give you [Dawson] any more benefits that other
4 advertisers and make myself look bad in the process.

- 5 - On or about November 19, 1999, a post to the Internet by "DR7" [Menard]
6 provides instructions to remedy problem of member who received an AVR2
7 [smart card replacement] and programmer [device used to program smart
8 cards or illegal substitute cards] and was unable to load properly. "DR7's"
9 [Menard's] instructions include, "using DOS talk v1.7 and loading the
10 avr2e3m [EchoStar] file which allows AVR2 to use the 3M keys from
11 wintalk."
12
- 13 - 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
15 slave who can count clock cycles and perform a high glitch on vcc/clk given
16 a command from the PC. All that is required to fix the current situation is a
17 new .exe file given different glitches to the card."
- 18 - On or about December 17, 1999, a post to the Internet by "Nipper-Clauz"
19 [Tarnovsky], entitled "Twas the Night Before Christmas," provided EchoStar
20 Bat keys.
- 21 - On or about December 20, 1999, a post to the Internet by "Nipper-Clauz"
22 [Tarnovsky] entitled "'tis the season to be jolly," provided additional
23 EchoStar Bat keys.
- 24 - On or about December 21, 1999, a post to the Internet by "Nipper-Clauz"
25 [Tarnovsky] entitled "be merry harry," provided even more EchoStar Bat
26 keys.
- 27 - On or about February 2, 2000, Dawson and Discount Satellite were raided a
28 second time by the RCMP after local reports regarding Dawson's continued
selling of pirated DSS and EchoStar access cards and other illegal signal theft
devices on the Internet through his website, www.discountsatellite.com.
- On or about February 25, 2000, a post by "NiPpEr" [Tarnovsky] to the
internet states providing EchoStar Bat keys.
- On or about March 24, 2000, a post to the internet by "xbr21" [Tarnovsky]
providing EchoStar Bat keys.

- 1 - On or about March 29, 2000, DirecTV executed and seized Dawson's
2 business in satisfaction of the judgment obtained by DirecTV against
3 Dawson. Shortly thereafter, Dawson posted a public statement on his
4 website, www.discountsatellite.com, regarding the status of his business's
5 operations. Included in this statement, Dawson provided a link to
6 www.DSScanada.com, another website owned, operated, and maintained by
7 Dawson. Through this website, Dawson continued to solicit business from
8 his large customer base in addition to new customers.
- 9 - On or about May 5, 2000, an NDS Memorandum captioned "Report Week
10 18", concerning NDS agent Christopher Tarnvosky, states in relevant part:
11 "You will note that suspicion has fallen on MIKE [Tarnovsky]...There are a
12 series of threatening statements inasmuch that MIKE [Tarnovsky] is behind
13 DR7 [Allen Menard and the website www.dr7.com] and therefore MIKE
14 [Tarnovsky] hacked EHOSTAR etc, etc."
- 15 - On or about June 21, 2000, a post to the Internet by "Hitec" [Quinn],
16 concerning "Koin" [Sergei], states "[f]or the time being... I am removing all
17 dealer links from the site... Koin is closing the website but still accepting
18 orders at Koin@koinvision.com . . . now its cash (no money orders at all) and
19 no site.... Any other files that are required to help out the Koinster will be
20 posted here from now on."
- 21 - On or about June 27, 2000, a post to the Internet by "Hitec" [Quinn],
22 concerning business operations of Koin [Sergei], stating "Koin [Sergei] is
23 closing the website but still accepting orders at Koin@Koinvision.com . . .
24 My self I personally vouch for Koin and his support. Even with his one
25 complaint the guy has to admit that Koin did send his package originally
26 (although it was seized) and he did make up for it after a couple of weeks . . .
27 Any other files that are required to help out the Koinster will be posted here
28 [www.hitecsat.com] from now on." A later post on the same date by "Hitec"
[Quinn] stating "as I already said . . . no money order now and only email . . .
I will post any files needed to help out Koin [Sergei]. His email addy again
is Koin@koinvizion.com."
- On or about August 15, 2000, a post by "HeeD" states "the group that is
supporting DN E3M [the illegal DISH Network hack] has proven that they
know this system inside-and-out. They are not just taking stabs in the dark,
or speculating about things...they actually know!"
- On or about September 19, 2000, it was discovered that Tarnovsky placed
approximately 80 phone calls to Israel [NDS] and 120 to Belgium.

1 Tarnovsky also traveled over seas twice every six months going to Brussels
2 and other European countries. Tarnovsky had received two parcels at his
3 residence from Minnesota and Virginia [Tarnovsky Sr.].

- 4 - On or about November 21, 2000, a post to the Internet by “Koinvizion”
5 [Sergei] announcing that [Defendants] can now fix the “smartcard not
6 inserted correctly Error for \$50.00USD per card + the usual shipping charges
7 for everyone.”
- 8 - On or about December 23, 2000, a post by “xbr21” [Tarnovsky], responding
9 to invitation by other members wishing “Nipper Clauze” [Tarnovsky] would
10 reappear and provide information, and states “you want nipper clauze
11 [Tarnovsky] here,” and then states “there will be no boxes anymore! There
12 will be no more fights amongst us. Learn from this and prosper. Works
13 across the world! Do the following: get atr, wait 500ms to ensure card is idle.
14 Send this packet to 288-02 or equivalent ROM 3 nagra cam! Rx 4+4096
15 bytes and you have entire eeprom. Send this, then rx 4 bytes + 4096 bytes of
16 eeprom.” The post was signed by “nipper clause 00” [Tarnovsky]. This
17 December 23, 2000 post by Tarnovsky provided hackers around the world
18 the ‘road map’ and instructional code to effectuate a complete dump of
19 Plaintiffs’ entire EEPROM Code.
- 20 - On December 24, 2000, a post to the Internet by “Nipper 2000” [Tarnovsky]
21 at 3:26 a.m. publishing the FULL Echo ROM Code on www.piratesden.com,
22 Discussion Forum. “Nipper 2000’s” [Tarnovsky’s] post, entitled “tHe ReAl
23 V3 DuMp!,” stating “tHeRe WiLl bE nO bOxEs aNyMoRe! tHeRe WiLl bE
24 nO mOrE flgHtInG aMoNgSt uS. LeArN fRoM ThIs aNd pRosPer. tHiS
25 WiLl Be PoStEd To ALl NeWsGrOuPs ArOuNd ThE WoRlD! ThIs Is
26 Dr7’S cOdE (WeSt 3M v3) tHe rEaL sTuFf!!” Tarnovsky then goes on to
27 state: “I wILL dUmP ALL vErSiOnS oF tHe WeSt CoDe LoOk FoR iT hErE!
28 nlpPeR cLaUz 00” [Tarnovsky].
- 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].
- On or about May 18, 2001, a post to the Internet by “Hitec” [Quinn],
responding to “Kelly’s” [Menard’s] allegations, stating “if I was involved in
the Echostar hack I would have forced the price down to an affordable rate
instead of lying to dealers and constantly gouging them. If memory serves

1 me correctly I even advertised for the competition that did force the price
2 down considerably.”

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

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

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

19 346. The multiple acts of racketeering activity as set forth above by
20 Defendants Norris, Hasak, Tarnovsky, Kommerling, Luyando, among others, were
21 interrelated, part of a common and continuous pattern of fraudulent schemes, and
22 perpetrated for the same or similar purposes, thus constituting a “pattern of
23 racketeering activity,” as defined in 18 U.S.C. § 1961(5).

24 347. By reason of these circumstances and events, Defendants Norris,
25 Hasak, Tarnovsky, Kommerling, Luyando, among others, have agreed to conduct
26 and participate, directly and indirectly, in the conduct of the affairs of the enterprise
27 through a pattern of racketeering activity, in violation of 18 U.S.C. § 1962(c).

28 348. Defendants’ violations have injured and will continue to injure
EchoStar by depriving them of subscription and pay-per-view revenues and other
valuable consideration, compromising EchoStar’s security and accounting systems,

1 infringing on EchoStar's trade secrets and proprietary information, interfering with
2 EchoStar's contractual and prospective business relations, and damaging Plaintiffs'
3 reputation in the DBS industry resulting in, among other injuries, irreparable harm
4 to the commercial goodwill that Plaintiffs have established in the relevant market
5 place.

6 **TENTH CAUSE OF ACTION**

7 **(RICO, 18 U.S.C. § 1962(d))**

8 349. Plaintiffs re-allege and incorporate the above as if fully set forth in this
9 cause of action.

10 350. By reason of these circumstances and events, Defendants, as persons
11 within the meaning of 18 U.S.C. § 1962(3), along with other unknown, unlawfully,
12 willfully, and knowingly conspired and agreed to conduct and participate, directly
13 and indirectly, in the conduct of the affairs of the enterprise through a pattern of
14 racketeering activity, in violation of 18 U.S.C. § 1962(d).

15 351. Defendants' violations have injured and will continue to injure
16 EchoStar by depriving them of subscription and pay-per-view revenues and other
17 valuable consideration, compromising EchoStar's security and accounting systems,
18 infringing on EchoStar's trade secrets and proprietary information, interfering with
19 EchoStar's contractual and prospective business relations, and damaging Plaintiffs'
20 reputation in the DBS industry resulting in, among other injuries, irreparable harm
21 to the commercial goodwill of Plaintiffs that has been established in the relevant
22 market place.

23 **ELEVENTH CAUSE OF ACTION**

24 **(Unauthorized Interception, Receipt, and Use of a Multichannel Video or** 25 **Information Provider's Programs or Services in Violation of California Penal** 26 **Code § 593d(a))**

27 352. Plaintiffs re-allege and incorporate the above as if fully set forth in this
28 cause of action.

1 353. Defendants, individually and as members of the conspiracy, were and
2 are actively engaged in the business of knowingly and willfully making and
3 maintaining unauthorized connections EchoStar's system, in violation of California
4 Penal Code § 593d(a)(1).

5 354. Defendants, individually and as members of the conspiracy, were and
6 are actively engaged in the business of knowingly and willfully purchasing,
7 possessing, attaching, causing to be attached, assisting others in attaching, and
8 maintaining the attachment of unauthorized devices to EchoStar's satellite system
9 including, but not limited to, Pirated EchoStar Access Cards and other
10 circumvention or signal theft devices designed to enable users to illegally modify or
11 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
12 limited to, loaders, dead processor boot boards, glitches, bootloaders, unloopers,
13 emulators, printed circuit boards, programmers, integrated receivers/decoders,
14 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
15 Locks, and/or other hardware and software intended for the unlawful and
16 unauthorized modification of and/or access to EchoStar's digital satellite system),
17 in violation of California Penal Code § 593d(a)(2).

18 355. Defendants, individually and as members of the conspiracy, were and
19 are actively engaged in the business of knowingly and willfully making and
20 maintaining the modification and alteration to EchoStar's satellite system, in
21 violation of California Penal Code § 593d(a)(3).

22 356. Defendants, individually and as members of the conspiracy, were and
23 are actively engaged in the business of knowingly and willfully making and
24 maintaining modifications and alterations to EchoStar's Access Cards and
25 obtaining Pirated EchoStar Access Cards and other circumvention or signal theft
26 devices designed to enable users to illegally modify or alter EchoStar Access Cards
27 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
28 processor boot boards, glitches, bootloaders, unloopers, emulators, printed circuit

1 boards, programmers, integrated receivers/decoders, Audio Video Replicators
2 “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
3 and software intended for the unlawful and unauthorized modification of and/or
4 access to EchoStar’s digital satellite system) knowing, or having reason to know,
5 that Pirated EchoStar Access Cards and other circumvention or signal theft devices
6 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
7 Plaintiffs’ Security System (including, but not limited to, loaders, dead processor
8 boot boards, glitches, bootloaders, unloopers, emulators, printed circuit boards,
9 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”
10 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
11 software intended for the unlawful and unauthorized modification of and/or access
12 to EchoStar’s digital satellite system) would be used, and were used, to obtain
13 EchoStar’s satellite television programming service without authorization by or
14 payment to EchoStar, in violation of California Penal Code § 593d(a)(4).

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

17 358. Defendants’ acts constituting violations of California Penal Code §§
18 593d(a)(1)-(4) have been and continue to be performed without the permission,
19 authorization, or consent of Plaintiffs.

20 359. 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.

25 360. Defendants’ violations of California Penal Code §§ 593d(a)(1)-(4)
26 were done knowingly and willfully, and for the purpose of commercial advantage
27 or private financial gain. EchoStar is entitled to recover, under California Penal
28 Code § 593d(f), the greater of three times its actual damages, or statutory damages

1 of \$5,000 for each violation of California Penal Code §§ 593d(a)(1)-(4). Plaintiffs
2 are also entitled to recover reasonable attorney's fees. California Penal Code §
3 593d(f)(2).

4 **TWELFTH CAUSE OF ACTION**
5 **(Manufacture, Advertisement, Possession, and Sale of Signal Theft Devices in**
6 **Violation of California Penal Code § 593d(b))**

7 361. Plaintiffs re-allege and incorporate the above as if fully set forth in this
8 cause of action.

9 362. Defendants, individually and as members of the conspiracy, were and
10 are actively engaged in the business of designing, manufacturing, assembling,
11 modifying, importing (to the United States), distributing, possessing, selling,
12 offering to sell, and advertising for sale Pirated EchoStar Access Cards and other
13 circumvention or signal theft devices designed to enable users to illegally modify or
14 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
15 limited to, loaders, dead processor boot boards, glitches, bootloaders, unloopers,
16 emulators, printed circuit boards, programmers, integrated receivers/decoders,
17 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
18 Locks, and/or other hardware and software intended for the unlawful and
19 unauthorized modification of and/or access to EchoStar's digital satellite system)
20 knowing, or having reason to know, that Pirated EchoStar Access Cards and other
21 circumvention or signal theft devices designed to enable users to illegally modify or
22 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
23 limited to, loaders, dead processor boot boards, glitches, bootloaders, unloopers,
24 emulators, printed circuit boards, programmers, integrated receivers/decoders,
25 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
26 Locks, and/or other hardware and software intended for the unlawful and
27 unauthorized modification of and/or access to EchoStar's digital satellite system)
28

1 were designed, in whole or in part, to decrypt, decode, descramble, or otherwise
2 make intelligible, EchoStar's satellite television programming service without
3 authorization by or payment to EchoStar, in violation of California Penal Code §
4 593d(b).

5 363. EchoStar is a "multichannel video or information provider" within the
6 meaning of California Penal Code § 593d(i).

7 364. EchoStar's satellite transmission of television programming is an
8 "encrypted, encoded, scrambled, or other nonstandard signal" within the meaning
9 of California Penal Code § 593d(b).

10 365. Defendants' acts constituting violations of California Penal Code §
11 593d(b) have been, and continue to be, performed without the permission,
12 authorization, or consent of Plaintiffs.

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

18 367. Defendants' violations of California Penal Code §§ 593d(b) were done
19 knowingly and willfully, and for the purpose of commercial advantage or private
20 financial gain.

21 368. EchoStar is entitled to recover, under California Penal Code § 593d(f),
22 the greater of three times its actual damages, or statutory damages of \$5,000 for
23 each violation of California Penal Code §§ 593d(b). Plaintiffs are also entitled to
24 recover reasonable attorney's fees. California Penal Code § 593d(f)(2).

25 **THIRTEENTH CAUSE OF ACTION**
26 **(Unauthorized Connection to a Multichannel Video or Information Provider's**
27 **System in Violation of California Penal Code § 593d(c))**
28

1 369. Plaintiffs re-allege and incorporate the above as if fully set forth in this
2 cause of action.

3 370. Defendants, individually and as members of the conspiracy, were and
4 are actively engaged in the business of making and maintaining unauthorized
5 connections, attaching, causing to be attached, assisting others in attaching, and
6 maintaining attachments to EchoStar's satellite system for the purpose of
7 interfering with, altering, and degrading EchoStar's satellite service and for
8 transmitting or broadcasting EchoStar's satellite television program service, in
9 violation of California Penal Code § 593d(c).

10 371. EchoStar is a "multichannel video or information provider" within the
11 meaning of California Penal Code § 593d(i).

12 372. Defendants' acts constituting violations of California Penal Code §§
13 593d(c) have been, and continue to be, performed without the permission,
14 authorization, or consent of Plaintiffs.

15 373. 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.

20 374. Defendants' violations of California Penal Code §§ 593d(c) were done
21 knowingly and willfully, and for the purpose of commercial advantage or private
22 financial gain.

23 375. EchoStar is entitled to recover, under California Penal Code § 593d(f),
24 the greater of three times its actual damages, or statutory damages of \$5,000 for
25 each violation of California Penal Code §§ 593d(c). Plaintiffs are also entitled to
26 recover reasonable attorney's fees. California Penal Code § 593d(f)(2).
27
28

1 **FOURTEENTH CAUSE OF ACTION**
2 **(Manufacture and Sale of Pirate Access Cards**
3 **in Violation of California Penal Code § 593e(a))**

4 376. Plaintiffs re-allege and incorporate the above as if fully set forth in this
5 cause of action.

6 377. Defendants, individually and as members of the conspiracy, made and
7 maintained unauthorized connections for the purpose of intercepting, receiving, and
8 using programs or other services carried by EchoStar.

9 378. Defendants, individually and as members of the conspiracy, purchased,
10 possessed, attached, caused to be attached, and/or assisted others in maintaining the
11 attachment of unauthorized Pirated EchoStar Access Cards and other circumvention
12 or signal theft devices designed to enable users to illegally modify or alter EchoStar
13 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
14 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
15 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
16 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
17 other hardware and software intended for the unlawful and unauthorized
18 modification of and/or access to EchoStar's digital satellite system) to receive
19 EchoStar's satellite television programming broadcasts and transmissions, for the
20 purpose of intercepting, receiving, and using EchoStar's satellite television
21 programs and services carried on the DISH Network, in violation of California
22 Penal Code § 593e(b).

23 379. Defendants, individually and as members of the conspiracy, made and
24 maintained modifications and alterations to Pirated EchoStar Access Cards and
25 other circumvention or signal theft devices designed to enable users to illegally
26 modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
27 (including, but not limited to, loaders, dead processor boot boards, glitchers,
28

1 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
2 receivers/decoders, Audio Video Replicators “AVRs,” AVR wafers, ATMEGA
3 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
4 unlawful and unauthorized modification of and/or access to EchoStar’s digital
5 satellite system) for the purpose of intercepting, receiving, and using EchoStar’s
6 satellite television programs and services carried on the DISH Network, in violation
7 of California Penal Code § 593e(b).

8 380. EchoStar is a “subscription television system” within the meaning of
9 California Penal Code § 593e(f).

10 381. Defendants’ acts constituting violations of California Penal Code §
11 593e(a) have been, and continue to be, performed without the permission,
12 authorization, or consent of Plaintiffs.

13 382. Due to Defendants’ wrongful conduct, Plaintiffs are entitled, under
14 California Penal Code § 593e(c), to the amount of the value of the connection and
15 subscription fee service actually charged by EchoStar for the period of unauthorized
16 use which is an amount to be proven at trial. Plaintiffs are also entitled, under
17 California Penal Code § 593e(d), to its full costs plus an award of reasonable
18 attorney’s fees.

19 **FIFTEENTH CAUSE OF ACTION**
20 **(Manufacture and Sale of Pirate Access Cards**
21 **in Violation of California Penal Code § 593e(b))**

22 383. Plaintiffs re-allege and incorporate the above as if fully set forth in this
23 cause of action.

24 384. Defendants, individually and as members of the conspiracy, were and
25 are actively engaged in the business of designing, manufacturing, assembling,
26 modifying, importing (to the United States), distributing, possessing, selling,
27 offering to sell, and advertising for sale Pirated EchoStar Access Cards and other
28

1 circumvention or signal theft devices designed to enable users to illegally modify or
2 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
3 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
4 emulators, printed circuit boards, programmers, integrated receivers/decoders,
5 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
6 Locks, and/or other hardware and software intended for the unlawful and
7 unauthorized modification of and/or access to EchoStar's digital satellite system)
8 knowing, or having reason to know, that Pirated EchoStar Access Cards and other
9 circumvention or signal theft devices designed to enable users to illegally modify or
10 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
11 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
12 emulators, printed circuit boards, programmers, integrated receivers/decoders,
13 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
14 Locks, and/or other hardware and software intended for the unlawful and
15 unauthorized modification of and/or access to EchoStar's digital satellite system)
16 were designed, in whole or in part, to decrypt, decode, descramble, or otherwise
17 make intelligible, EchoStar's satellite television programming service without
18 authorization by or payment to EchoStar, in violation of California Penal Code §
19 593e(b).

20 385. EchoStar is a "subscription television system" within the meaning of
21 California Penal Code § 593h(1).

22 386. EchoStar's satellite transmission of television programming is an
23 "encoded, scrambled, or other nonstandard signal" within the meaning of California
24 Penal Code § 593e(g).

25 387. Defendants' acts constituting violations of California Penal Code §
26 593e(b) have been, and continue to be, performed without the permission,
27 authorization, or consent of Plaintiffs.

28

1 388. Defendants' violations have injured, and will continue to injure,
2 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
3 other valuable consideration, compromising Plaintiffs' security and accounting
4 systems, infringing Plaintiffs' trade secrets and proprietary information, and
5 interfering with Plaintiffs' contractual and prospective business relations.

6 389. Defendants' violations of California Penal Code § 593e(b) were
7 committed knowingly and willfully, and for the purpose of commercial advantage
8 or private financial gain.

9 390. Due to Defendants' wrongful conduct, Plaintiffs are entitled, under
10 California Penal Code § 593e(c), to either: statutory damages in an aggregate
11 amount of not less than \$500 or more than \$10,000 for each device, plan, or kit for
12 a device, or for a printed circuit manufactured, imported, assembled, sold, offered
13 for sale, possessed, advertised for sale, or otherwise provided in violation of
14 California Penal Code § 593e(b) (California Penal Code § 593e(c)(1)); or three
15 times the amount of actual damages sustained by Plaintiffs as a result of
16 Defendants' violations of California Penal Code § 593e(b) and any revenues which
17 have been obtained by Defendants as a result of Defendants' violations of
18 California Penal Code § 593e(b), or an amount equal to three times the value of the
19 services unlawfully obtained by Defendants, or the sum of \$500 for each
20 unauthorized signal theft device manufactured, sold, used, or distributed.
21 (California Penal Code § 593e(c)(2)).

22 391. Because of Defendants' violations of California Penal Code § 593e(c)
23 were committed knowingly and willfully and for purposes of commercial advantage
24 or private financial gain, the Court may increase the award of damages, whether
25 actual or statutory, by an amount of not more than \$50,000. Because of Defendants'
26 violations of California Penal Code § 593e(c) were committed knowingly, willfully,
27 and wantonly, punitive damages are appropriate, under California Penal Code §
28

1 593e(c)(2). Plaintiffs are also entitled, under California Penal Code § 593e(d), to
2 its full costs plus an award of reasonable attorney's fees.

3 **SIXTEENTH CAUSE OF ACTION**

4 **(Unfair Competition, Cal. Bus. & Prof. Code § 17200)**

5 392. Plaintiffs re-allege and incorporate the above as if fully set forth in this
6 cause of action.

7 393. Defendants and/or their agents have engaged in unfair competition in
8 violation of California Business and Professions Code Sections 17200 et seq. Such
9 violations caused injury to Plaintiffs in the district, elsewhere through the State of
10 California, the United States and elsewhere. Defendants willfully, unlawfully, and
11 according to a plan, with the intention of harming Plaintiffs, acquired EchoStar
12 Access Cards. Defendants violated those cards using expensive equipment, cracked
13 the Access Cards and the Security Systems, and extracted and copied Plaintiffs'
14 proprietary software and code. After transferring the code to NDS Americas, Inc.
15 in California, Defendants caused it to be disseminated over the Internet to facilitate
16 further copying. This lead to the production of altered Access Cards on a large
17 scale to the detriment of Plaintiffs' business and its reputation among its customers
18 and in the industry. Defendants' engaged in further unlawful conduct through
19 utilizing the supposed security flaws in Plaintiffs technology to compete with
20 Plaintiffs. This conduct constitutes an unlawful, unfair, and fraudulent business act
21 or practice within the meaning of Section 17200.

22 394. Defendants' invasive attack of EchoSar's Access Cards, dissemination
23 of the information about the Security System and assistance to Menard and his
24 network of distributors was intentional and done for the wrongful purpose of
25 inhibiting competition in the industry and unfairly benefiting Defendants. As a
26 direct and proximate result of Defendants' violations of Section 17200, Defendants
27 have been unjustly enriched at Plaintiffs' expense. Defendants' and/or their agents
28 have taken money from Plaintiffs in the form of lost business opportunity from

1 subscription sales to persons that, instead, used pirated Access Cards to receive
2 DISH Network programming without paying the subscription price. Plaintiffs
3 therefore have an ownership in the unjust profits received by Defendants and/or
4 their agents. Plaintiffs are entitled to disgorgement of all monies unlawfully earned
5 and restitution of any and all of Plaintiffs' property, including Access Cards,
6 unlawfully obtained or possessed by Defendants and/or their agents.

7 395. Based upon information and belief, Defendants and/or their agents
8 committed the acts described in this Amended Complaint, including
9 misappropriating Plaintiffs' trade secrets, injuring Plaintiffs, violating the Digital
10 Millennium Copyright Act, and illegally cracking Plaintiffs' Security System, in,
11 amongst other place, the State of California and in Israel.

12 396. The acts alleged herein constitute unlawful, unfair, and fraudulent
13 business acts or practices within the meaning of Section 17200.

14 397. As a direct and proximate result of Defendants' violations of Section
15 17200, Plaintiffs have suffered and will continue to suffer irreparable harm,
16 including but not limited to harm to their business reputations, and goodwill.
17 Therefore, Plaintiffs' remedy at law is inadequate and Plaintiffs are entitled to an
18 injunction prohibiting Defendants from taking any steps to contribute to the
19 copying of any of Plaintiffs' software code or any steps to reverse engineer or
20 otherwise violate a technological measure on any EchoStar Access Card, as well as
21 other remedies to which Plaintiffs may prove themselves entitled.

22 SEVENTEENTH CAUSE OF ACTION

23 (Tortious Interference with Contractual Relations)

24 398. Plaintiffs re-allege and incorporate the above as if fully set forth in this
25 cause of action.

26 399. Defendants have intentionally and knowingly interfered with the
27 contractual relations between EchoStar and its DISH Network subscribers by
28 inducing, procuring, conspiring, and aiding and abetting an as yet undetermined

1 number of DISH Network subscribers not to perform their respective contracts with
2 EchoStar by designing, developing, manufacturing, assembling, modifying,
3 importing (to the United States), exporting, trafficking, selling, and otherwise
4 distributing Pirated EchoStar Access Cards and other circumvention or signal theft
5 devices designed to enable users to illegally modify or alter EchoStar Access Cards
6 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
7 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
8 boards, programmers, integrated receivers/decoders, Audio Video Replicators
9 "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
10 and software intended for the unlawful and unauthorized modification of and/or
11 access to EchoStar's digital satellite system) to DISH Network subscribers, and
12 advertising and providing software, information, and technical support services
13 relating to Pirated EchoStar Access Cards and other circumvention or signal theft
14 devices designed to enable users to illegally modify or alter EchoStar Access Cards
15 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
16 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
17 boards, programmers, integrated receivers/decoders, Audio Video Replicators
18 "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
19 and software intended for the unlawful and unauthorized modification of and/or
20 access to EchoStar's digital satellite system) to DISH Network subscribers thereby
21 causing the breach or termination of DISH Network subscribers' accounts resulting
22 in damage to EchoStar.

23 400. Defendants have interfered with the contractual relations between
24 EchoStar and its DISH Network subscribers without justification or legal excuse.
25 Defendants' interference was willful, wanton, and malicious.

26 401. Defendants' conduct has injured and will continue to injure Plaintiffs
27 by depriving Plaintiffs of subscription and pay-per-view revenues and other
28 valuable consideration.

1 402. Due to Defendants' wrongful conduct, Defendants are liable for all
2 pecuniary losses suffered by Plaintiffs as a result of Defendants' interference, and
3 for punitive damages.

4 **EIGHTEENTH CAUSE OF ACTION**

5 **(Tortious Interference with Prospective Contractual Relations)**

6 403. Plaintiffs re-allege and incorporate the above as if fully set forth in this
7 cause of action.

8 404. Defendants have intentionally and knowingly interfered with
9 EchoStar's business of selling its satellite television programming services to
10 prospective DISH Network subscribers, and selling additional programming
11 services to existing DISH Network subscribers, by providing Pirated EchoStar
12 Access Cards and other circumvention or signal theft devices designed to enable
13 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security
14 System (including, but not limited to, loaders, dead processor boot boards,
15 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
16 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
17 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
18 for the unlawful and unauthorized modification of and/or access to EchoStar's
19 digital satellite system), and advertising and providing software, information, and
20 technical support services relating to Pirated EchoStar Access Cards and other
21 circumvention or signal theft devices designed to enable users to illegally modify or
22 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
23 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
24 emulators, printed circuit boards, programmers, integrated receivers/decoders,
25 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
26 Locks, and/or other hardware and software intended for the unlawful and
27 unauthorized modification of and/or access to EchoStar's digital satellite system) to
28

1 an as yet undetermined number of DISH Network subscribers and prospective
2 subscribers, thereby hindering EchoStar from acquiring such prospective relations.

3 405. Defendants' intentional acts were designed to disrupt the relationships
4 EchoStar has with current and prospective DISH Network subscribers. Defendants'
5 motive and purpose was to effectuate and/or assist others in effectuating a wide
6 spread compromise of Plaintiffs' conditional access system for commercial
7 advantage in the satellite encryption industry.

8 406. Such intentional acts proximately caused economic harm to Plaintiffs
9 by depriving Plaintiffs of subscription and pay-per-view revenues and other
10 valuable consideration of current and prospective DISH Network subscribers.

11 407. Defendants engaged in conduct that was unlawful, tortious and
12 otherwise wrongful under Plaintiffs' other causes of action as alleged herein.

13 408. Due to Defendants' wrongful conduct, Defendants are liable for all
14 pecuniary losses suffered by Plaintiffs as a result of Defendants' interference, and
15 for punitive damages.

16 NINETEENTH CAUSE OF ACTION

17 (Unjust Enrichment)

18 409. Plaintiffs re-allege and incorporate the above as if fully set forth in this
19 cause of action.

20 410. Defendants have usurped for themselves, as well as assisting others in
21 usurping trade secrets, proprietary information, revenues, programming, and other
22 property rights belonging to Plaintiffs for the purpose of, among others, enhancing
23 the commercial value of Defendants' goods and services by effectuating and
24 assisting others in effectuating a wide spread compromise of Plaintiffs' conditional
25 access system.

26 411. Plaintiffs are informed and believe that Defendants are still currently
27 in possession of: (a) Plaintiffs' proprietary information including but not limited to
28 proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or

1 other proprietary information unlawfully extracted from the microprocessor
2 embedded in Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated
3 EchoStar Access Cards and/or other circumvention or signal theft devices designed
4 to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs'
5 Security System (including, but not limited to, loaders, dead processor boot boards,
6 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
7 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
8 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
9 for the unlawful and unauthorized modification of and/or access to EchoStar's
10 digital satellite system); and/or (c) monies or other proceeds unlawfully obtained
11 through the sale/distribution of, or assistance or support provided in connection
12 with, among others, Pirated EchoStar Access Cards and/or other circumvention or
13 signal theft devices designed to enable users to illegally modify or alter EchoStar
14 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
15 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
16 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
17 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
18 other hardware and software intended for the unlawful and unauthorized
19 modification of and/or access to EchoStar's digital satellite system).

20 412. As a direct and proximate result of their unlawful and improper acts,
21 Defendants have been unjustly enriched and Plaintiffs have suffered, and will
22 continue to suffer, loss of profits, among others, by virtue of Defendants' conduct.
23 The exact amount of unjust profits realized by Defendants, and profits lost by
24 Plaintiffs, are presently unknown to Plaintiffs and cannot be readily ascertained
25 without an accounting.

26 413. Defendants' unlawful sale of Pirated EchoStar Access Cards and other
27 circumvention or signal theft devices designed to enable users to illegally modify or
28 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not

1 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
2 emulators, printed circuit boards, programmers, integrated receivers/decoders,
3 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
4 Locks, and/or other hardware and software intended for the unlawful and
5 unauthorized modification of and/or access to EchoStar's digital satellite system),
6 and Defendants' usurpation of Plaintiffs' trade secrets, proprietary information,
7 revenues, programming and other property rights belonging to Plaintiffs, is causing,
8 and will continue to cause, irreparable injury to Plaintiffs unless Defendants are
9 preliminarily and permanently restrained and enjoined from this activity.

10 414. Plaintiffs are, therefore, entitled to a preliminary and permanent
11 injunction restraining and enjoining Defendants and their employees, agents, and
12 representatives, and all persons acting thereunder, in concert with, or on their
13 behalf, from selling pirated, modified, and/or counterfeit EchoStar Access Cards.
14 Plaintiffs are further entitled to economic damages in the forms of disgorgement
15 and/or restitution for all benefits unjustly received, retained and/or appropriated by
16 Defendants, as well as exemplary damages for Defendants' intentional, willful and
17 malicious conduct.

18 TWENTIETH CAUSE OF ACTION

19 (Conversion)

20 415. Plaintiffs re-allege and incorporate the above as if fully set forth in this
21 cause of action.

22 416. By virtue of the conduct set forth herein, Defendants have unlawfully
23 converted, and are continuing to convert and assist others in converting Plaintiffs'
24 property, namely EchoStar Access Cards, the proprietary information contained
25 therein, and the DISH Network programming that Plaintiffs' conditional access
26 system is employed to protect, for their own personal and commercial use, benefit
27 and gain.

28

1 417. Such conversion was and is substantial and unwarranted and done
2 intentionally and wrongfully by Defendants to deprive Plaintiffs of their proprietary
3 interests, economic interests and commercial goodwill, and for Defendants' direct
4 benefit and advantage.

5 418. Due to Defendants' wrongful conversion and disposition of EchoStar's
6 satellite television programming services, Plaintiffs have suffered, and continue to
7 suffer substantial damages.

8 TWENTY-FIRST CAUSE OF ACTION

9 (Negligent Hiring, Training, Retention and/or Supervision)

10 419. Plaintiffs re-allege and incorporate the above as if fully set forth in this
11 cause of action.

12 420. NDS had a duty to investigate the backgrounds of persons NDS
13 considered hiring for employment. Prior to NDS hiring or establishing an agency
14 relationship with Norris, Hasak, Kommerling, Luyando, Donev, Nedeltchev,
15 Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky
16 Sr., Sommerfield and Bruce, among others, to act for and at the direction and under
17 the control of NDS, NDS knew¹⁸ or had reason to know that these individual were
18 well-known hackers in the pirate world or otherwise posed a risk of injury to,
19 among others, Plaintiffs. NDS knew or had reason to know, or failed to use
20 reasonable care to discover the unfitness of Norris, Hasak, Kommerling, Luyando,
21 Donev, Nedeltchev, Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei,
22 Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce, among others before hiring
23 them for legitimate employment due to their colorful past in the pirate world and
24 the personal connections these individual defendants maintained up through the
25 time NDS hired them and at all times subsequent thereto. NDS knew or had reason
26 to know facts which would warn a reasonable person that these individual

27 _____
28 ¹⁸ In fact, it was Tarnovsky's status as a satellite hacker/pirate that prompted NDS to hire him in the first place.

1 defendants presented an undue risk of harm to third persons in *light of the*
2 *particular work they would be performing*. Due to their known involvement in
3 hacking, NDS risked that these individual defendants would act in conformity with
4 their past reputation and character.

5 421. NDS breached its duty of care by, *inter alia*: (a) failure to use ordinary
6 care in the selection and hiring of Norris, Hasak, Kommerling, Luyando, Donev,
7 Nedeltchev, Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei, Dale,
8 Frost, Tarnovsky Sr., Sommerfield and Bruce, among others; (b) failure to use
9 ordinary in establishing rules, regulations and/or policies for Norris, Hasak,
10 Kommerling, Luyando, Donev, Nedeltchev, Tarnovsky, Menard, Wilson, Main,
11 Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce,
12 among others to follow; (c) failure to take reasonable precautions to prevent
13 negligent, reckless, wonton, willful, intentional and/or careless conduct by Norris,
14 Hasak, Kommerling, Luyando, Donev, Nedeltchev, Tarnovsky, Menard, Wilson,
15 Main, Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce,
16 among others; (d) failure to use ordinary care in the supervision of the activities
17 and conduct of Norris, Hasak, Kommerling, Luyando, Donev, Nedeltchev,
18 Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky
19 Sr., Sommerfield and Bruce, among others; (e) failure to use ordinary care to
20 prevent Norris, Hasak, Kommerling, Luyando, Donev, Nedeltchev, Tarnovsky,
21 Menard, Wilson, Main, Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky Sr.,
22 Sommerfield and Bruce, among others from causing an unreasonable risk of injury
23 to Plaintiffs; (f) failure to use ordinary care in exercising the degree of control it
24 retained, either directly or indirectly, over Norris, Hasak, Kommerling, Luyando,
25 Donev, Nedeltchev, Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei,
26 Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce, among others; (g) failure to
27 use ordinary care in the retention of Norris, Hasak, Kommerling, Luyando, Donev,
28 Nedeltchev, Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei, Dale,

1 Frost, Tarnovsky Sr., Sommerfield and Bruce, among others, once NDS knew, or in
2 the exercise of reasonable care should have known that these individual defendants
3 were engaging in unlawfull anticompetitive conduct; (h) failure to use ordinary
4 care to avoid and/or prevent Norris, Hasak, Kommerling, Luyando, Donev,
5 Nedeltchev, Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei, Dale,
6 Frost, Tarnovsky Sr., Sommerfield and Bruce, among others from creating a
7 foreseeable risk of injury to Plaintiffs; (i) failure to take affirmative action to
8 control or avoid increasing the danger from conduct which Norris, Hasak,
9 Kommerling, Luyando, Donev, Nedeltchev, Tarnovsky, Menard, Wilson, Main,
10 Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce,
11 among others at least partially created; and/or (j) in the event NDS contends that it
12 obtained Plaintiffs' proprietary conditional access Codes through 'reverse
13 engineering'¹⁹, failure to use ordinary care by providing, or allowing Norris, Hasak,
14 Kommerling, Luyando, Donev, Nedeltchev, Tarnovsky, Menard, Wilson, Main,
15 Dawson, Quinn, Sergei, Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce,
16 among others to obtain and subsequently misuse this proprietary information. As a
17 direct and proximate cause of NDS's negligence as described in (a) through (j)
18 above, Plaintiffs have suffered and will continue to suffer substantial damage and
19 injury.

20 422. The acts and/or omissions of Norris, Hasak, Kommerling, Luyando,
21 Donev, Nedeltchev, Tarnovsky, Menard, Wilson, Main, Dawson, Quinn, Sergei,
22 Dale, Frost, Tarnovsky Sr., Sommerfield and Bruce, among others, forming the
23 basis of Plaintiffs' Second Amended Complaint, injured and will continue to injure
24 Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and
25 other valuable consideration, compromising Plaintiffs' security and accounting
26 systems, infringing Plaintiffs' trade secrets and proprietary information, interfering

27 ¹⁹ As stated herein, however, Plaintiffs are informed and believe NDS did not obtain Plaintiffs'
28 proprietary information through a lawful manner and, as such, any potential claim by NDS of
'reverse engineering' is inapposite and should not insulate NDS from liability for its wrongdoing.

1 with Plaintiffs' contractual and prospective business relations and damaging the
2 commercial reputation and good will Plaintiffs have established in the conditional
3 access system and direct-to-home satellite television market places. Additionally,
4 these unlawful and anticompetitive acts and/or omissions have resulted in
5 Plaintiffs' having to expend substantial economic resources to combat the NDS
6 controlled and facilitated compromise of Plaintiffs' conditional access system that
7 Plaintiffs would not have otherwise been forced to expend.

8 TWENTY-SECOND CAUSE OF ACTION

9 (Breach of Contract)

10 423. Plaintiffs re-allege and incorporate the above as if fully set forth in this
11 cause of action.

12 424. On or about November 6, 1998, Defendant George Tarnovsky
13 activated services with Plaintiffs on a 3500 model JVC DISH Network receiver,
14 which he purchased from Sears and Roebuck. As part of this transaction Defendant
15 agreed to be bound by Plaintiffs' Residential Subscriber Agreement ("Agreement").

16 425. On or about August 3, 1999, Christopher Tarnovsky purchased a
17 Webstar, model number 7120, DISH Network receiver from Fry's Electronics and
18 activated its programming on August 3, 1999. Additionally, as part of this
19 transaction Defendant also agreed to be bound by Plaintiffs' Residential Subscriber
20 Agreement.

21 426. Pursuant to the Agreement, Plaintiffs granted Defendants a license to
22 use of Plaintiffs' smart card(s), in which legal title was retained with Plaintiffs. In
23 relevant part, the parties' Agreement states that "DISH DBS Smart Cards are
24 [EchoStar's] property and any tampering or other unauthorized modification to the
25 Smart Card may result in, and subject you to, legal action." Further the Agreement
26 states "[s]mart cards are not transferable. Your Smart Card will only work in the
27 DISH Network receiver to which it was assigned by DISH Network."
28

1 427. Concerning Defendants efforts to hack and circumvent Plaintiffs'
2 Smart Cards as alleged in Plaintiffs' Second Amended Complaint and incorporated
3 by reference as if stated fully herein, the Agreement specifically provided that
4 Defendants would not reverse engineer or tamper with Plaintiffs' smart cards:

5
6 Your DISH Network receiver contains certain
7 components and software which are proprietary to DISH
8 Network. *You agree that you will not try to reverse
9 engineer decompile or disassemble any software or
10 hardware contained within your receiver or our Smart
11 Card. Such actions are strictly prohibited and may
12 result in the termination of your Services and/or legal
13 action.* (Emphasis added).

14 428. Plaintiffs are informed and believe that Defendants have illegally, and
15 in breach of the parties' Agreement, reverse engineered and/or hacked Plaintiffs'
16 smart cards. Concerning piracy of Plaintiffs' smart cards, the Agreement further
17 provides:

18 **WARNING AGAINST PIRACY:** *It is a violation of
19 several federal and state laws to receive any Services, or
20 any portion of such Services, without paying for them.
21 The penalty for violating such laws can range from
22 imprisonment to civil damages awards of up to \$110,000
23 per violation.*

24 429. All conditions precedent have been performed by or have occurred as
25 required by Plaintiffs' Agreement and by applicable law. Plaintiffs have performed
26 their obligations under the Agreement and have provided Defendants the Services
27 they contracted for.

28 430. Defendants, however, Plaintiffs are informed and believe as pleaded
herein, have not performed their contractual obligations per the Agreement.

 431. As a proximate result of Defendants' breach, Plaintiffs have suffered
the damages, including but not limited to, loss of net profits, damages for exposure
of Plaintiffs' EEPROM over the internet, disclosure of Plaintiffs' ROM code as

1 facilitated by Defendants' illegal actions which were in breach of the parties'
2 agreement.

3 432. Also as a proximate result of Defendants' conduct, it has become
4 necessary for Plaintiffs' to retain the undersigned counsel in order to prosecute this
5 litigation and seek reimbursement for their reasonable and necessary attorney's fees
6 as authorized by the Agreement, and for all damages allowable by law.

7 433. Concerning Plaintiffs' recovery of attorney fees, the Agreement
8 specifically states, "if we [Plaintiffs] use . . . an attorney to collect money you owe
9 us or to assert any other right which we may have against you, you agree to pay the
10 reasonable costs of collection or other action. These costs might include, but are
11 not limited to, ... reasonable attorneys fees and court costs."

12 TWENTY-THIRD CAUSE OF ACTION

13 (Civil Conspiracy)

14 434. Plaintiffs re-allege and incorporate the above as if fully set forth in this
15 cause of action.

16 435. The Defendants and/or their agents have conspired with each other and
17 others working in concert with them to achieve an unlawful goal by unlawful
18 means. Specifically, the Defendants and/or their agents as well as others acting in
19 concert therewith, have conspired and agreed to restrain competition in the market
20 for conditional access systems related to transmission of satellite signals, by
21 unlawfully (a) effectuating and facilitating others in effectuating a wide spread
22 compromise EchoStar's conditional access system, (b) altering, pirating, modifying,
23 compromising, and/or counterfeiting EchoStar Access Cards, (c) distributing
24 Pirated EchoStar Access Cards and other circumvention or signal theft devices
25 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
26 Plaintiffs' Security System (including, but not limited to, loaders, dead processor
27 boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards,
28 programmers, integrated receivers/decoders, Audio Video Replicators "AVRs,"

1 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
2 software intended for the unlawful and unauthorized modification of and/or access
3 to EchoStar's digital satellite system), and (d) advertising and providing software,
4 information, and technical support services relating to Pirated EchoStar Access
5 Cards and other circumvention or signal theft devices designed to enable users to
6 illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
7 (including, but not limited to, loaders, dead processor boot boards, glitchers,
8 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
9 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
10 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
11 unlawful and unauthorized modification of and/or access to EchoStar's digital
12 satellite system) into the stream of interstate and foreign commerce.

13 436. The objective of Defendants and/or their agents' conspiracy was
14 unlawfully attempting to hinder and damage a major competitor in the market place
15 (of which Defendants were a participant) because, among other things, NDS was on
16 the verge of losing a valuable contact to supply encryption technology to DirecTV,
17 its major client, who was in the process of negotiating/investigating the conditional
18 access system licensed by NagraStar to EchoStar.

19 437. Defendants knew, or should have known, that designing,
20 manufacturing, assembling, modifying, importing (to the United States), exporting,
21 selling, and otherwise distributing Pirated EchoStar Access Cards and other
22 circumvention or signal theft devices designed to enable users to illegally modify or
23 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
24 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
25 emulators, printed circuit boards, programmers, integrated receivers/decoders,
26 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
27 Locks, and/or other hardware and software intended for the unlawful and
28

1 unauthorized modification of and/or access to EchoStar's digital satellite system)
2 was and is illegal and prohibited.

3 438. The wrongs and tortious conduct flowing from Defendants' conspiracy
4 include, *inter alia*, misappropriating Plaintiffs' trade secrets, injuring Plaintiffs,
5 violating the Digital Millennium Copyright Act, and illegally hacking Plaintiffs'
6 Security System, in addition to committing the other torts and violations set forth in
7 each separate cause of action in Plaintiffs' Second Amended Complaint.

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

13 **PRAYER FOR RELIEF**

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

15 A. Find that Defendants' conduct in designing, developing, manufacturing,
16 assembling, modifying, importing (to the United States), exporting, trafficking,
17 distributing, and selling Pirated EchoStar Access Cards and other circumvention or
18 signal theft devices designed to enable users to illegally modify or alter EchoStar
19 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
20 loaders, dead processor boot boards, glitches, bootloaders, unloopers, emulators,
21 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
22 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
23 other hardware and software intended for the unlawful and unauthorized
24 modification of and/or access to EchoStar's digital satellite system), placing
25 advertisements for the sale of such Pirated EchoStar Access Cards and other
26 circumvention or signal theft devices designed to enable users to illegally modify or
27 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
28 limited to, loaders, dead processor boot boards, glitches, bootloaders, unloopers,

1 emulators, printed circuit boards, programmers, integrated receivers/decoders,
2 Audio Video Replicators “AVRs,” AVR wafers, ATMEGA 128s, JTAGs, Digi-
3 Locks, and/or other hardware and software intended for the unlawful and
4 unauthorized modification of and/or access to EchoStar’s digital satellite system),
5 or providing software, information, and technical support services relating to
6 Pirated EchoStar Access Cards and other circumvention or signal theft devices
7 designed to enable users to illegally modify or alter EchoStar Access Cards and/or
8 Plaintiffs’ Security System (including, but not limited to, loaders, dead processor
9 boot boards, glitches, bootloaders, unloopers, emulators, printed circuit boards,
10 programmers, integrated receivers/decoders, Audio Video Replicators “AVRs,”
11 AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and
12 software intended for the unlawful and unauthorized modification of and/or access
13 to EchoStar’s digital satellite system) intended to facilitate the illegal and
14 unauthorized reception and use of EchoStar’s satellite television programming
15 services by persons not authorized to receive such programming violates 47 U.S.C.
16 §§ 605(a) and 605(e)(4), 18 U.S.C. §§ 2511(1)(a) and (c), 18 U.S.C. §§ 1962(c) and
17 1962(d), 15 U.S.C. §§ 1114 and 1125(a), California Penal Code §§ 593(d)(a)(1)-
18 (4), 593e(b), and 593e(c), California Business and Professions Code § 17200, and
19 California state law;

20 B. Find further that Defendants’ violations were willful, for a tortious or illegal
21 purpose, or for purposes of direct or indirect commercial advantage or private
22 financial gain;

23 C. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), 17 U.S.C. § 1203(b)(1), 18
24 U.S.C. § 2520(b)(1), 18 U.S.C. § 1964(a), 15 U.S.C. § 1116, California Penal Code
25 §§ 593d(g) and 593e(e), California Business and Professions Code § 17206, and
26 California state law, enjoin and restrain Defendants and persons or entities
27 controlled directly or indirectly by Defendants from: (a) designing, manufacturing,
28 assembling, modifying, importing (to the United States), trafficking, possessing,

1 distributing, or selling Pirated EchoStar Access Cards and other circumvention or
2 signal theft devices designed to enable users to illegally modify or alter EchoStar
3 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
4 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
5 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
6 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
7 other hardware and software intended for the unlawful and unauthorized
8 modification of and/or access to EchoStar's digital satellite system); (b) assisting,
9 procuring, or aiding and abetting third persons in the unauthorized reception and
10 use of EchoStar's satellite television programming; (c) placing advertisements for
11 the sale of Pirated EchoStar Access Cards or other circumvention or signal theft
12 devices designed to enable users to illegally modify or alter EchoStar Access Cards
13 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
14 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
15 boards, programmers, integrated receivers/decoders, Audio Video Replicators
16 "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
17 and software intended for the unlawful and unauthorized modification of and/or
18 access to EchoStar's digital satellite system); or (d) providing software,
19 information, or technical support services relating to (1) Pirated EchoStar Access
20 Cards, (2) other circumvention or signal theft devices designed to enable users to
21 illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
22 (including, but not limited to, loaders, dead processor boot boards, glitchers,
23 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
24 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
25 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
26 unlawful and unauthorized modification of and/or access to EchoStar's digital
27 satellite system), or (3) the illegal and unauthorized reception and use of EchoStar's
28

1 satellite television programming service by persons not authorized to receive such
2 programming;

3 D. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), 18 U.S.C. § 2520(b)(1),
4 California Penal Code §§ 593d(g) and 593e(e), and California Business &
5 Professions Code § 17206, grant an Order directing Defendants to return to
6 Plaintiffs all trade secrets, proprietary information, Pirated EchoStar Access Cards,
7 other circumvention or signal theft devices designed to enable users to illegally
8 modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
9 (including, but not limited to, loaders, dead processor boot boards, glitches,
10 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
11 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
12 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
13 unlawful and unauthorized modification of and/or access to EchoStar's digital
14 satellite system), and any other hardware or software derived from EchoStar Access
15 Cards, Security System, or satellite television programming system;

16 E. In accordance with 47 U.S.C. § 605(e)(3)(B)(i), 18 U.S.C. § 2520(b)(1),
17 California Penal Code §§ 593d(g) and 593e(e), and California Business &
18 Professions Code § 17206, grant an Order impounding all Pirated EchoStar Access
19 Cards and other circumvention or signal theft devices designed to enable users to
20 illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security System
21 (including, but not limited to, loaders, dead processor boot boards, glitches,
22 bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated
23 receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA
24 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the
25 unlawful and unauthorized modification of and/or access to EchoStar's digital
26 satellite system) in the possession, custody, or control of Defendants, or related
27 entities of Defendants, that the Court has reasonable cause to believe were involved
28 in a violation of any causes of action alleged herein;

1 F. Grant an Order requiring Defendants to post a prominent public notice on
2 any Internet website owned, operated, maintained by Defendants notifying all
3 persons in possession of Pirated EchoStar Access Cards or other circumvention or
4 signal theft devices designed to enable users to illegally modify or alter EchoStar
5 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
6 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
7 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
8 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
9 other hardware and software intended for the unlawful and unauthorized
10 modification of and/or access to EchoStar's digital satellite system) that the cards
11 and devices have been recalled and that they must send the cards or devices to
12 EchoStar or destroyed;

13 G. Grant an Order requiring Defendants to identify all John Does working in
14 concert with Defendants in performing the unlawful acts described herein, and to
15 use all contact information in Defendants' possession, custody, or control to notify
16 anyone who has obtained a Pirated EchoStar Access Cards or other circumvention
17 or signal theft devices designed to enable users to illegally modify or alter EchoStar
18 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
19 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
20 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
21 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
22 other hardware and software intended for the unlawful and unauthorized
23 modification of and/or access to EchoStar's digital satellite system) from
24 Defendants that the cards and devices have been recalled and that they must send
25 the cards or devices to EchoStar or destroyed;

26 H. Grant an Order directing Defendants to preserve and maintain all records, in
27 any form (including electronic form), that evidences, refers to, or relates to: (a)
28 EchoStar Access Cards; (b) Plaintiffs' encryption technology; (c) Pirated EchoStar

1 Access Cards; (d) other circumvention or signal theft devices designed to enable
2 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security
3 System (including, but not limited to, loaders, dead processor boot boards,
4 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
5 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
6 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
7 for the unlawful and unauthorized modification of and/or access to EchoStar's
8 digital satellite system); (e) communications or correspondence with manufacturers,
9 suppliers, distributors, or customers of Pirated EchoStar Access Cards or other
10 circumvention or signal theft devices designed to enable users to illegally modify or
11 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
12 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
13 emulators, printed circuit boards, programmers, integrated receivers/decoders,
14 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
15 Locks, and/or other hardware and software intended for the unlawful and
16 unauthorized modification of and/or access to EchoStar's digital satellite system),
17 or access card programming services; (f) the identity of any manufacturers,
18 suppliers, distributors, or customers of Pirated EchoStar Access Cards or other
19 circumvention or signal theft devices designed to enable users to illegally modify or
20 alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not
21 limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers,
22 emulators, printed circuit boards, programmers, integrated receivers/decoders,
23 Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-
24 Locks, and/or other hardware and software intended for the unlawful and
25 unauthorized modification of and/or access to EchoStar's digital satellite system);
26 and (g) the quantity of Pirated EchoStar Access Cards, including EchoStar Access
27 Cards that have not yet been altered, pirated, modified, compromised, and/or
28 counterfeited, and other circumvention or signal theft devices designed to enable

1 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security
2 System (including, but not limited to, loaders, dead processor boot boards,
3 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
4 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
5 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
6 for the unlawful and unauthorized modification of and/or access to EchoStar's
7 digital satellite system) in inventory and sold by Defendants;

8 I. Grant an Order permitting Plaintiffs, through its counsel, to inspect and make
9 mirror image copies of any computer or electronic storage drives or back-up tapes
10 in the possession, custody, or control of Defendants or related entities that contain
11 information that evidences, refers to, or relates to Defendants' conduct of
12 designing, developing, manufacturing, assembling, modifying, importing (to the
13 United States), exporting, trafficking, distributing, and selling Pirated EchoStar
14 Access Cards or other circumvention or signal theft devices designed to enable
15 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security
16 System (including, but not limited to, loaders, dead processor boot boards,
17 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
18 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
19 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
20 for the unlawful and unauthorized modification of and/or access to EchoStar's
21 digital satellite system), or providing software, information, or technical support
22 services relating to Pirated EchoStar Access Cards or other circumvention or signal
23 theft devices designed to enable users to illegally modify or alter EchoStar Access
24 Cards and/or Plaintiffs' Security System (including, but not limited to, loaders,
25 dead processor boot boards, glitchers, bootloaders, unloopers, emulators, printed
26 circuit boards, programmers, integrated receivers/decoders, Audio Video
27 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
28 other hardware and software intended for the unlawful and unauthorized

1 modification of and/or access to EchoStar's digital satellite system) designed to
2 facilitate the illegal and unauthorized reception and use of satellite television
3 programming by persons not authorized to receive such programming;

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

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

13 L. In accordance with 47 U.S.C. §§ 605(e)(3)(C)(i), award Plaintiffs the greater
14 of (a) its actual damages together with any profits made by Defendants that are
15 attributable to the violation alleged herein, or (b) statutory damages in the amount
16 of up to \$100,000 for each violation of 47 U.S.C. § 605(e)(4);

17 M. In accordance with 18 U.S.C. § 2520(c)(2), award Plaintiffs the greater of (a)
18 its actual damages together with any profits made by Defendants as a result of the
19 violations alleged herein, or (b) statutory damages of which is the greater of \$100
20 per day for each day of violation of 18 U.S.C. §§ 2511(1) or \$10,000;

21 N. In accordance with California Penal Code § 593d(f), award Plaintiffs the
22 greater of (a) three times its actual damages, or (b) statutory damages or \$5,000 for
23 each violation of California Penal Code §§ 593d(a)(1)-(4) and 593d;

24 O. In accordance with California Penal Code § 593e(c)(1), award Plaintiffs the
25 greater of (a) three times its actual damages and any revenues obtained by
26 Defendants as a result of Defendants' violations, (b) three times the value of the
27 services unlawfully obtained, or (c) the sum of \$500 for each Pirated EchoStar
28 Access Cards or other circumvention or signal theft devices designed to enable

1 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security
2 System (including, but not limited to, loaders, dead processor boot boards,
3 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
4 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
5 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
6 for the unlawful and unauthorized modification of and/or access to EchoStar's
7 digital satellite system) that was manufactured, sold, used, or distributed by
8 Defendants;

9 P. In accordance with California Penal Code § 593e(c)(1), award Plaintiffs
10 statutory damages in the amount of up to \$10,000 for each violation of California
11 Penal Code § 593e(b);

12 Q. In accordance with 18 U.S.C. § 1964(c), award Plaintiffs treble the amount of
13 actual damages suffered by Plaintiffs in their business or property by reason of
14 Defendants' violations of 18 U.S.C. §§ 1964(c) and 1962(d);

15 R. In accordance with 15 U.S.C. § 1117, award Plaintiffs treble the amount of
16 actual damages suffered by Plaintiffs;

17 S. In accordance with 18 U.S.C. § 2520(b)(2) and California Penal Code §
18 593e(c)(1), award Plaintiffs punitive damages for each violation of 18 U.S.C. §§
19 2511(1) and California Penal Code § 593e(b), respectively;

20 T. In accordance with California state law, award Plaintiffs compensatory
21 damages, in an amount to be proved at trial, and punitive damages for each of the
22 claims arising under state law;

23 U. In accordance with California state law, Order an accounting, establish a
24 constructive trust in favor of Plaintiffs, and direct Defendants to disgorge all profits
25 obtained by them as a result of: (a) designing, manufacturing, assembling,
26 modifying, importing (to the United States), trafficking, possessing, distributing, or
27 selling Pirated EchoStar Access Cards or other circumvention or signal theft
28 devices designed to enable users to illegally modify or alter EchoStar Access Cards

1 and/or Plaintiffs' Security System (including, but not limited to, loaders, dead
2 processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit
3 boards, programmers, integrated receivers/decoders, Audio Video Replicators
4 "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware
5 and software intended for the unlawful and unauthorized modification of and/or
6 access to EchoStar's digital satellite system); (b) providing software, information,
7 or technical support services relating to: (1) altering, pirating, modifying,
8 compromising, and/or counterfeiting EchoStar Access Cards; (2) Pirated EchoStar
9 Access Cards; (3) other circumvention or signal theft devices designed to enable
10 users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security
11 System (including, but not limited to, loaders, dead processor boot boards,
12 glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers,
13 integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers,
14 ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended
15 for the unlawful and unauthorized modification of and/or access to EchoStar's
16 digital satellite system); or (4) the illegal and unauthorized reception and use of
17 EchoStar's satellite television programming by persons not authorized to receive
18 such programming; (c) assisting, procuring, or aiding and abetting third persons in
19 the unauthorized reception and use of EchoStar's satellite television programming;
20 or (d) advertising the sale of Pirated EchoStar Access Cards or other circumvention
21 or signal theft devices designed to enable users to illegally modify or alter EchoStar
22 Access Cards and/or Plaintiffs' Security System (including, but not limited to,
23 loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators,
24 printed circuit boards, programmers, integrated receivers/decoders, Audio Video
25 Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or
26 other hardware and software intended for the unlawful and unauthorized
27 modification of and/or access to EchoStar's digital satellite system);
28

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

DEMAND FOR JURY TRIAL

Plaintiffs EchoStar Communications Corporation, EchoStar Satellite Corporation, and EchoStar Technologies Corporation (collectively, "EchoStar") and NagraStar L.L.C. hereby demand trial by jury in this action.

DATED: February 18, 2004

Respectfully Submitted,

SQUIRE, SANDERS & DEMPSEY L.L.P.

By: Cynthia A. Ricketts
Cynthia A. Ricketts
Attorneys for Plaintiffs
ECHOSTAR SATELLITE CORPORATION,
ECHOSTAR COMMUNICATIONS CORPORATION,
ECHOSTAR TECHNOLOGIES CORPORATION,
AND NAGRASTAR L.L.C.

1 V. In accordance with 47 U.S.C. § 605(e)(3)(B)(iii), 18 U.S.C. § 2520(b)(3), 18
2 U.S.C. § 1964(c), and California Penal Code §§ 593d(f)(2) and 593e(d), direct
3 Defendants to pay Plaintiffs all of Plaintiffs' costs, reasonable attorneys' fees, and
4 investigative fees;

5 W. For pre-judgment interest on all damages, where allowable by law;

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

7 Y. For such additional relief as the Court deems to be just and equitable.

8
9 Dated: February 18, 2004

10 SQUIRE, SANDERS & DEMPSEY L.L.P.

11
12 By: Cynthia A. Ricketts /msr
13 Cynthia A. Ricketts
14 Attorneys for Plaintiffs
15 ECHOSTAR SATELLITE CORPORATION,
16 ECHOSTAR COMMUNICATIONS
CORPORATION,
17 ECHOSTAR TECHNOLOGIES CORPORATION,
18 AND NAGRASTAR L.L.C.

19 Of Counsel

20 T. WADE WELCH & ASSOCIATES
21 T. Wade Welch (*pro hac vice*)
22 Ross W. Wooten (*pro hac vice*)
23 Chad M. Hagan (*pro hac vice to be filed*)
24 2401 Fountainview Suite 700
25 Houston, Texas 77057
26 Telephone: (713) 952-4334
27 Facsimile: (713) 952-4994
28

REC'D

FAX NO. :

09 Apr. 2002 18:43 P2

1 JAMES A. DiBOISE, State Bar No. 083296
 2 ELIZABETH M. SAUNDERS, State Bar No. 138249
 3 WILSON SONSINI GOODRICH & ROSATI
 Professional Corporation
 4 650 Page Mill Road
 Palo Alto, CA 94304-1050
 Telephone: (650) 493-9300
 Facsimile: (650) 565-5100
 5
 Attorneys for Plaintiffs
 6 GROUPE CANAL+ S.A.,
 CANAL+ TECHNOLOGIES, S.A. and
 7 CANAL+ TECHNOLOGIES, INC.

8 UNITED STATES DISTRICT COURT
 9 NORTHERN DISTRICT OF CALIFORNIA
 10 SAN FRANCISCO DIVISION

12 GROUPE CANAL+ S.A., CANAL+)	CASE NO.: C02-01178 VRW
13 TECHNOLOGIES, S.A., CANAL+)	
14 TECHNOLOGIES, INC.,)	DECLARATION OF OLIVER
Plaintiffs,)	KÖMMERLING IN SUPPORT OF
)	PLAINTIFFS' MOTION FOR
)	EXPEDITED DISCOVERY AND TO
)	PRESERVE DOCUMENTS AND
16 v.)	THINGS
17 NDS GROUP PLC, NDS AMERICAS, INC.,)	
Defendants.)	Date: April 18, 2002
)	Time: 2:00 p.m.
)	Place: Courtroom 6, 17 th Floor
)	
)	
)	

22 I, Oliver Kömmerling, declare as follows:

23 1. I am the same Oliver Kömmerling that Mr. Peled identifies in his declaration
 24 submitted in this action. I am the principal shareholder of ADSR, a company that provides
 25 security services to many different businesses. I have provided and continue to provide security
 26 services to both Canal+ and to NDS Group

27 2. I have read Mr. Peled's declaration and disagree with several of the
 28 statements he makes in it and disagree with some of those statements that he attributes to me.

KÖMMERLING DECLARATION
 No. C02-01178 VRW

FAX NO. :

FAX NO. :

09 Apr. 2002 16:44 P3

1 3. I have met with Canal+' lawyers at their request and discussed my knowledge
 2 regarding NDS activities concerning the publication of Canal+' smart card software on the website
 3 "DR7" in March 1999. I have through my lawyer made NDS aware that I am prepared to meet
 4 their lawyers also to discuss my knowledge of this matter. I wish to tell the truth concerning what I
 5 know of this matter and would respond to a subpoena to testify issued by this Court in connection
 6 with Canal+' lawsuit against NDS. As long as my costs were paid, it would not be a burden to me
 7 to appear in the United States for a deposition.

8 4. I am fearful that pressure will be brought to bear on me and my friends by NDS to
 9 not testify in this action. NDS' lawyer has already spoken with my lawyer, telling him that I
 10 should be reminded that I am under contractual obligations to NDS not to divulge any confidential
 11 information of NDS. I do not believe that my knowledge of this matter is of a nature that is
 12 subject to any such confidentiality agreement with NDS. I was asked to come to a meeting in
 13 New York City on Tuesday 9th or Wednesday 10th April 2002 by lawyers working for NDS and
 14 News Corporation along with all the other NDS people identified by Canal+ for deposition. I
 15 declined to attend that meeting, but did make NDS aware that I was prepared to meet with their
 16 lawyers in London.

17 5. I am also fearful that this action will be damaging to the reputation of my company
 18 ADSR, of which I hold 60% of the shares and NDS holds 40%. I have provided services to both
 19 NDS and Canal+, as well as other third parties, for the past two years. This action has, however,
 20 led to some of ADSR's other customers expressing concern at the ability of ADSR to maintain
 21 confidentiality given that NDS is a shareholder. In addition, Mr. Peled, through an NDS employee,
 22 has informed me that I must not continue providing services to Canal+ if this action proceeds. As
 23 a result, I am seeking to terminate the joint venture with NDS and have offered to acquire their
 24 40% shareholding. They have refused to sell their shares while this action proceeds. The fact that I
 25 have knowledge of NDS' activities concerning the publication of the Canal+ smartcard software
 26 means that this action also involves me. I want to testify to tell the truth regarding my knowledge
 27 of this matter in a fair proceeding with both sides present in order that I may be done with this
 28

178

FROM :

FAX NO. :

09 Apr. 2002 18:44 P4

1 matter so I may take such steps as are necessary to preserve the reputation of ADSR or, if
2 appropriate, to set up a new business independent of NDS.

3 6. I have provided consultancy services in the field of microelectronics and software
4 security to NDS since mid-1996. I have also provided consultancy services to and worked closely
5 with NDS operational security department helping to defeat piracy during the same period. I was
6 instrumental in the establishment of the NDS research facility in Haifa, Israel in late 1996 and
7 early 1997 and the recruitment of engineers for that facility. I was responsible for the training of
8 all the engineers in Haifa at that time.

9 7. Based on my personal knowledge and on information and belief from conversations
10 with people who were involved in the events, I understand the following to be true:

11 a. NDS engineers in the NDS facility in Haifa, Israel obtained Canal+ smart cards
12 and using the techniques taught by me (some of which were described in my paper "Design
13 Principles for Tamper Resistant Smartcards" written with Markus Kuhn) were able to physically
14 extract the Canal+ machine code embedded in their smart cards.

15 b. NDS engineers disassembled and analyzed the extracted machine code and
16 were then able to explore methods by which people would be able to circumvent the security
17 measures contained within that machine code.

18 c. These efforts and the results were put into a written document and circulated
19 among some NDS employees. I am also in possession of a copy of this report.

20 d. I was informed by a friend of the publication of the Canal+ code on the DR7
21 website. It became apparent to me that it was the same code that had been extracted and analyzed
22 in the NDS Haifa laboratories. Subsequently, I was able to confirm this fact with no reasonable
23 doubt in my mind.

24 e. Later I was told by then current NDS employees that the Canal+ code was
25 either handed to or sent from Israel to Southern California to Chris Tarnovsky. The same NDS
26 employees told me that it was agreed that Chris Tarnovsky should arrange for the Canal+ code to
27 be published on the internet.

28

KOMMERLING DECLARATION
NO. C02-01178 VRW

-3-

179

FROM :

FAX NO. :

09 Apr. 2002 18:45 PS

1 f. In a telephone conversation with Ms. Genie Gavenchak, a lawyer for News
 2 Corporation, I said that I believed the factual allegations in the Canal+ complaint were accurate
 3 and truthful. I also told Ms. Gavenchak that I had told all these facts to Mr. Peled. I had done this
 4 at a private dinner with him in late 1999.

5 8. I have read the allegations contained in paragraph 17 of Mr. Peled's declaration and
 6 say the following:

7 a. I did inform Mr. Peled that ADSR would be undertaking work for Canal+ on its
 8 smart card security measures as I was required to under the terms of the agreement between ADSR
 9 and NDS. I informed Mr. Peled in his capacity as a director of ADSR.

10 b. I informed Mr. Peled that Canal+ had supplied me with a development version
 11 of a type of chip which was one of several candidates for use in their latest generation cards and
 12 that Canal+ had asked me to test the security features, not that I had been supplied with a
 13 development version of the latest generation card. I told Mr. Peled that the security features of that
 14 particular chip were not sufficient to use the card for their conditional access system because I
 15 broke those security features in days. I informed Mr. Peled that I had recommended a different,
 16 more secure microprocessor be used. I did not tell him the type to be used, only that minor
 17 customization would be necessary to satisfy me that the security features would be adequate. I
 18 made no comment to Mr. Peled regarding the new generation card itself.

19 c. I never stated to Mr. Peled that Canal+' security measures and smart card were
 20 not state of the art, nor would I, as that would have required me to breach my confidentiality
 21 obligations to Canal+. I do not know why Mr. Peled chose to attribute those statements to me as I
 22 never made them to him. I would question the use of the phrase "state of the art" by Mr. Peled
 23 given that I have much more knowledge of the respective technology employed by NDS and
 24 Canal+ than he has. I do not believe that it is possible to make any reasonable judgment on
 25 whether a chip or card is state of the art or not given the limited information I gave to Mr. Peled
 26 about the work I was undertaking on behalf of Canal+.

27
28


180

FROM :

FAX NO. :

09 Apr. 2002 18:45 P6

1 I declare under penalty of perjury under the laws of the United States of America that the
 2 foregoing is true and correct. Executed on 9 April 2002, in London, England.

3
 4 

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

181

1 JAMES A. DiBOISE, State Bar No. 083296
ELIZABETH M. SAUNDERS, State Bar No. 138249
2 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
3 650 Page Mill Road
Palo Alto, CA 94304-1050
4 Telephone: (650) 493-9300
Facsimile: (650) 565-5100

5 Attorneys for Plaintiffs
6 GROUPE CANAL+ S.A.,
CANAL+ TECHNOLOGIES, S.A. and
7 CANAL+ TECHNOLOGIES, INC.

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

12 GROUPE CANAL+ S.A., CANAL+) CASE NO.: C02-01178 VRW
13 TECHNOLOGIES, S.A., CANAL+)
14 TECHNOLOGIES, INC.,)
Plaintiffs,)
15 v.)
16 NDS GROUP PLC. NDS AMERICAS, INC.,)
17 Defendants.)
18 Date: April 18, 2002
19 Time: 2:00 p.m.
20 Place: Courtroom 6, 17th Floor
21)

22 I, Jan Saggiori, declare as follows:

23 1. I am employed by SSS LLC, based in Geneva, Switzerland. SSS Llc is
24 engaged in providing consulting services to Canal+ in the area of conditional access systems for
25 digital TV.

26 2. I have known Chris Tarnovsky since the mid-1990s and have had various
27 email exchanges with him concerning digital television and security measures used to protect
28 those signals. I met Chris via the internet and a user group called TV-Crypt Group. TV-Crypt

SAGGIORI DECLARATION
No. C02-01178 VRW

1 Group was managed by Markus Kuhn when Markus was a student at the University of Erlangen
2 in Germany. While Chris was living in Germany , he and I exchanged email messages and
3 exchanged software concerning D2MAC-Eurocrypt (Canal+/TV1000) and Videocrypt
4 (Sky/Filmnet) systems. Chris went back to the United States but we continued our email
5 correspondence. Chris began to study the Videoguard system (version P1) utilized by DirecTV
6 in the United States to protect its satellite TV signals. Chris asked me for some source code I
7 had written concerning the DES encryption algorithm and associated tables.

8 3. In 1997 Chris contacted me and requested that I put him in contact with
9 people who were able to analyze smart cards. I introduced Chris to Vesselin Ivanov Nedeltchev
10 ("Vesco") and gave Vesco's phone number to Chris. Vesco is an engineer I had met in Geneva
11 who had studied smart cards and their associated security systems. I also met Vesco in mid-2001
12 in Geneva when he came to see me specifically to discuss questions related to the security
13 encryption of access control systems and at that time I understood Vesco was working directly
14 for Reuven Hasak of NDS.

15 4. Very shortly after its publication on the DR7 website, I became aware that
16 the Canal+ smart card code was available for downloading from the DR7 website. I downloaded
17 that smart card code from the DR7 website and examined that binary code and the text files
18 included with it. The text document indicated that the code associated with the EEPROM had
19 been lost during the extraction process but indicated that the rest of the data from the user-ROM
20 was included in the file. I examined that binary code and determined that the code present at the
21 2000 address was missing.

22 5. Knowing that Chris Tarnovsky knew Al Menart because I had introduced
23 the two of them in 1996 and knowing that Al Menart was the Webmaster of DR7, I asked Chris
24 Tarnovsky if he could obtain the [missing] code present at the 2000 address from Al Menart. By
25 an email exchange from Chris Tarnovsky, Chris sent me an 8kb binary file that he claimed
26 contained the requested code extracted from the Canal+ smart card. Attached as Exhibit A to
27 this declaration is a copy of the email I received from Chris Tarnovsky (using the alias of Arthur
28

BERKELEY SCIENTIFIC TRANSLATION SERVICE

voice 510 548-4665
fax 510 548-4666
web <http://www.berksci.com>
mail P.O. Box 150 Berkeley CA 94701

Date: April 10, 2002

Re: 25012.500

CERTIFICATION OF EDITING

This certifies that the editing and verification of the translation from French to English of the two French legal documents entitled: "DECLARATION OF JAN SAGGIORI IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED DISCOVERY AND TO PRESERVE DOCUMENTS AND THINGS" and: "DECLARATION OF VINCENT LABIE IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED DISCOVERY AND TO PRESERVE DOCUMENTS AND THINGS" have been performed by a qualified professional translator competent in both languages, and is an accurate and complete rendering of the content of the original document to the best of our ability.

Signed:



Marlo R. Martin, Ph.D.
Director

1 JAMES A. DiBOISE, State Bar No. 083296
ELIZABETH M. SAUNDERS, State Bar No. 138249
2 WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
3 650 Page Mill Road
Palo Alto, CA 94304-1050
4 Telephone: (650) 493-9300
Facsimile: (650) 565-5100

5 Attorneys for Plaintiffs
6 GROUPE CANAL+ S.A.,
CANAL+ TECHNOLOGIES, S.A. and
7 CANAL+ TECHNOLOGIES, INC.

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

12 GROUPE CANAL+ S.A., CANAL+
13 TECHNOLOGIES, S.A., CANAL+
TECHNOLOGIES, INC.,

14 Plaintiffs,

15 v.

16 NDS GROUP PLC, NDS AMERICAS, INC.,

17 Defendants.

) CASE NO.: C02-01178 VRW
)
)
) **DECLARATION OF JAN**
) **SAGGIORI IN SUPPORT OF**
) **PLAINTIFFS' MOTION FOR**
) **EXPEDITED DISCOVERY AND TO**
) **PRESERVE DOCUMENTS AND**
) **THINGS**

) Date: April 18, 2002
) Time: 2:00 p.m.
) Place: Courtroom 6, 17th Floor
)
)
)
)
)
)
)

22
23 Je soussigné Jan Saggiori, déclare ce qui suit :

24
25 1. Je suis employé par la société SSS Llc. basée à Genève, en Suisse. SSS Llc fournit des
26 services de consulting à Canal+ dans le domaine d'accès conditionnel pour la télévision
27 numérique.
28

-186

1
2 2. Je connais Chris Tarnovsky depuis le milieu des années 90 et nous avons échangé différents
3 email ayant trait à la télévision numérique et aux mesures de sécurité mises en œuvre pour
4 protéger les signaux. J'ai connu Chris à travers internet, et un groupe appelé « TV-Crypt ». Le
5 groupe « TV-Crypt » était géré par Markus Kuhn quand il était étudiant à l'université d'Erlangen
6 en Allemagne. Lorsqu'il vivait en Allemagne, Chris et moi avons échangé des E-mail et des
7 logiciels concernant les systèmes D2MAC-Eurocrypt (Canal+/TV1000) et Videocrypt
8 (Sky/Filmnet). Chris est rentré aux Etats-Unis et nous avons continué à correspondre par E-mail.
9 Chris commença à étudier les système Videoguard (version P1) utilisé par DirectTV aux Etats-
10 Unis pour protéger l'accès à ses signaux satellites. Chris me demanda du code source que j'avais
11 écrit et qui concernait l'algorithme de cryptage « DES » et les tables associées.
12
13

14
15 3. En 1997, Chris me contacta et me demanda de le mettre en contact avec des personnes
16 susceptibles d'analyser des cartes à puce. J'ai présenté à Chris Vesselin Ivanov Nedeltchev
17 (« Vesco ») et ai donné à Chris le numéro de téléphone de Vesco. Vesco est un ingénieur que j'ai
18 rencontré à Genève et qui avait étudié les cartes à puce et leur systèmes de sécurité. J'ai
19 également rencontré Vesco en mi 2001 à Genève quand il m'a contacté pour aborder en
20 particulier des questions relatives à la sécurité du cryptage de systèmes de contrôle d'accès ; à
21 cette époque, je compris que Vesco travaillait directement pour Reuven Hasak de NDS.
22

23 4. Très rapidement après sa publication sur le site web DR7, je fus informé qu'il était possible
24 de télécharger à partir du site DR7 le code de la carte à puce de Canal+. Je téléchargeai ce code
25 de la carte à puce à partir du site DR7 et examinai le code binaire ainsi que les fichiers textes
26 inclus. Le document texte indiquait que le code de l'EEPROM avait été perdu lors du processus
27 d'extraction mais précisait que le reste des données de la ROM utilisateur était présent dans le
28

- 187

1 fichier. J'examinai le code binaire et déterminai que le code présent à partir de l'adresse N°2000
2 était manquant.

3
4 5. Sachant que Chris Tarnovski connaissait Al Ménart parce que je les avait présentés en 1996 et
5 sachant qu'Al Ménart était le gestionnaire du site DR7, je demandai à Chris s'il pouvait obtenir
6 d'Al Ménart le code présent à partir de l'adresse N°2000. Par un échange d'Email, Chris
7 m'envoya un fichier binaire de 8 Kilo Octets qui contenait, m'assurait-il, le code réclamé extrait
8 de la carte à puce Canal+. Sont joints en annexe de cette présente déclaration, une copie de l'
9 Email reçu de Chris Tarnovski (qui utilisait le pseudonyme « Arthur von Neumann » ou
10 « Von ») en Annexe A et le code binaire transmis par cet Email en annexe B.
11
12

13
14 6. Plus tard en 1999, après que Chris m'eût rendu visite à Genève, nous discutâmes la possibilité
15 d'obtenir plus d'information concernant le composant Thomson utilisé dans les cartes à puce
16 Canal+. Chris m'envoya par Email un fichier qui contenait le manuel utilisateur du composant
17 Thomson. La page de garde du document que j'ai reçu de Chris est joint en annexe C de cette
18 présente déclaration. Le document reçu est une copie d'un manuel utilisateur confidentiel de
19 Thomson qu'il n'est possible d'obtenir de Thomson qu'à travers un strict accord de
20 confidentialité.
21

22 Je déclare, sous risque de poursuites selon les lois des Etats Unis d'Amérique, que ma présente
23 déclaration est exacte et sincère.

24
25 Signé : 8 Avril 2002, à Paris, France.
26
27

28 _____
/s/Jan Saggiori
Jan Saggiori

FROM: Arthur Von Neumann, INTERNET:von@metro2000.net
TO: SAGGIORI Jan, jan_saggiori
DATE: 28.03.99 13,36

Re: Re: Hi

Contents:

- 1 Internet Message Header
- 2 <no topic>

=====
Topic: Internet Message Header
=====

Sender: von@metro2000.net
Received: from relay1.smtp.psi.net (relay1.smtp.psi.net [38.8.14.2])
by hpdmgaaa.compuserve.com (8.8.8/8.8.8/HP-1.1) with ESMTP id NAA22853
for <jan_saggiori@compuserve.com>; Sun, 28 Mar 1999 13:36:11 -0500 (EST)
Received: from [38.223.67.2] (helo=ad2.com)
by relay1.smtp.psi.net with esmtp (Exim 1.90 #1)
for jan_saggiori@compuserve.com
id 10RKPX-00070z-00; Sun, 28 Mar 1999 13:36:17 -0500
Received: from hers (38.12.3.110) by ad2.com
with ESMTP (Apple Internet Mail Server 1.1.1); Sun, 28 Mar 1999 10:41:36 -0700
Message-Id: <4.2.0.25.19990328183134.00a377d0@metro2000.net>
X-Sender: von@metro2000.net
X-Mailer: QUALCOMM Windows Eudora Pro Version 4.2.0.25 (Beta)
Date: Sun, 28 Mar 1999 18:32:42 +0000
To: SAGGIORI Jan <jan_saggiori@compuserve.com>
From: Arthur Von Neumann <von@metro2000.net>
Subject: Re: Hi
In-Reply-To: <199903281247_MC2-6FBD-5DC0@compuserve.com>
Mime-Version: 1.0
Content-Type: multipart/mixed;
boundary="=====_6511890==_"

Good news from up north here.. Enjoy, keep for you please.. extremely top secret!

=====
Name: 16cf54.asc
=====

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hlwDwxweIrTEUX0BA/46bMvH26aivHISA7clOXn97JGt6hdy9xvUuiQX5EZVRtFy
BJWzMe0Vpq6VjUaJ+bWzrVo194CsndYT2/DjTfcP62FbXpEbiZgJUJkHd5xobp0
2DyMrRwY5s0Z+iLx1XF1PjQed5WeKcl/n1at0U8kkbfZlXhgoitJqbnWwqqYA
AA9gqCOcJAaevLvqyfigefbD1QfNkvrGPHIZHZQR/BdvZFHIZNyigKZpkGjuUhdC
dsIEuV0FDSEXG2R8gFOsMRnInj19Pn+GaG2ItMP2R6NGf5uxw2YPqvHCy/GXgdC
hpJ0SSSf7adrVEFjkHije3EXaSrRofXy2/QSgTM7/97DGcGeslZL7lCvL7K5Mfs
Nyoy559t7dqZgh1pdGUqtByg8i00M2Nr3sJ05T/T2HQiuqaSSK2F5J2jow3hWmL3
BgSlUeDUDuliteoXMNqF0Ued8KBaCM2hXVE1EsRm+RA4fovB3Ch3G/3YiRQhNZeLa
NPRclM0zNAU06QM9XKRfbaAQOpGoIJ2UR96+vL97snj4tem0/56bsZDs7Y5vNW+f
ZN3nTzkDTPV4+i+gDWbywN6xeVdfJBSN6WK0NUu4M8iEkqBul+kVBfeqmYVRvcuH
B3Oam7XvTtk34RXOSW9vi0ncw5DTxDuHXIVq/RCnxhscGNUECDTOzqfFwaYYSDBq
eNDW9F7BE+X+A/MHhFeGfN8cMBvuTlqLCUmehASwFBLZEpVn3ocOjr++nflBtocu
esCTkzhZjkYUeWkLoil1yk6nck8igL5KaLAUck0ZGGYsBQkF1XgkD3hOb1Q136Z
LT6harzhrL1MP7/QdtNbqsSj7xVfXJiHTThAKgm+4X21shF39m09Bz5r17yxpSz
F6aDsDBIm98JiFhaHMtFgQME4Rot2P4NZWE9R1joWcPG9uKwCFj14WYUVxsEbqo2
DrdsNv4PzG10Ji+KofEgq8bfHb4HVH+eykocQWo/B/kFkGppH6fK76ORnSK/5bJJ
LNkeM25OBq4O1103SFsTD4w8860ywfpcRJ2nYeZsm46C/6q4aE9G14EzZyM5kwei
nT8Ku27CUSirA6qJgBD8VtFY0rpTSAoly97pAk2PgoDbST8RaxyS+XK/EuvvTO
eLkHkRqeYVke6X6tNispJPQmDX1a61iB6+bAw7hqFPZ+JKV7E+zcXWmwrM4SkuWpm
IWnJqAwyp3W6ZEJSzojImdpV+OHDKjnGdmsjedqvZhkbsqUGOm270LGN5GHdMc
8xadFSjzgrvLIHRh9J27K8I2+K44BE8O/PLkrXkQDK/ERgYUF/IhKiuLaNjV6BU
Qvo11Y2tywUUJ+tdgfdVW7ps2KMfdewLnt56WSKR9KiZSIropXgpDwnlSOdCsEaa
s6Yul1q7z8yJw4MHUthZ8/dHi8uUqRGLexl/QTVWXN94F2Wb7ajBfXmZk+D7jQmb

EXHIBIT 2
Ech. A

189

VrOvkfhhZec68jhKr2YLU9ld+YG5hLREfl1r2T9NiYFBHa+AmJFTQlpxXrTbUQb
gXWrWX+SazO6G6sFWSYDpU7HxZ48yiZthc0P4Yy9aWxMa8tMcx1Lcjo/wN29QT9I
NKXCW2YX1X9MYYYZ6AD93Gx2aJk/v2afhtID/5PAC7C7WHqtq9L8CdL11hXUUVf
j2cdzcKjIETWSzBfEXWVvXE8wlonwzU100fKQxhwWUSq40TOqcR7+bPSQCPVaULK
ApyP8SikZYfSDEyT1IVfP6BXaWjPposgB5uNpads/D0BksqJ+8bPMFQ+kT9HBZIU
DymFZxO4xnbVJgpedjSljCxU7Kool7mKh7KumJ/yurC3V8nnbE/QsqOP7iHFZqb2
2qdtMqj2XODvHR5IZYsilHlfQSTu8xV9hmfYJV36sc93DPoLAtbSzYebwp1pDY
OKuBfexhFFmzL2Q7+DbV027IHMJ/SgcUlbeHfQcHh0fW9NK0GqcRM5x6i48SEPdD
Y19HxKWE3GG/Lv5RyRczvd8q7LXqW6Pc3c9wrxnLR+XC1EVEv6x1pFs3303TGNej
UddVXq4jhSi6CEjClvjW3HilzbgMvNi5cNLj2MWLXX6wpsDU6FHg2yww1aeW6Zs+
jT6UcNDznUMT/AlVmg9z6f0QEDHZ4FJqpcD9Exos1JMqBDZ6r2TO+DokLZELloQ
EcQp8EkQ34xU5vW4mndu5/RtUIWEA1PVDg+7GCI8fQMM8yb/MrpS6/oLAApLIsEc
pzh89XkfmMwMNBuX4NHZ4SRsGXzwmSgSIVJ3OjuxqeslAQjAZNHISOha98DSxshG
o1XrYfsh0/AsqJCb1xzCKA6i8j/Vu14hBGzILN8a5i5Xu6raC1hLWjoKGFuGEfP
2kVr7ifzibjJ4cCH5UG6wk5EJR5gBq5fL5KVnc+Fdzuo8opvZpkn3peRppLF/IO
+YTYfwuAMXNmYrkQC15tBFjAsD1X36B30ycXBf1GRAhPS/x3e6TEacsGNpitZxv
fQfOZbiKeE114A75/4Yzp8Hkh2FrKEL9PHV9AFEutyddtpSGPmovALw/lyv2P5es
NOmMq8SfWW/5FkdqP92Y/CO5Gjzsi3XqDbh8hB73/Isj0R+EN0CKTsCp/V8A1
IFP1LnLZ8E4tRQPEuAbQ9OvQIRln/ODG9BcC4K87uK8UmulYEPbTtEmwJE74eOK
KLSMcVwy8myEuQgg5q6vYu5RXcqTjFe+V7taWpRHKPFfJYcw/15EjTINt+6WIXQc
jJWDxthL7fLlvO+2yh+GTIyDEZ1x5M4q/ixEzN1ASaQc53fc9tle6sRrjQ/Dwq
sKalcha19/ju8OFkROaM95BfLfgqZFLiDuqACIplH2vQ0giCKM5xpV+7+q4+5RjA
6MS41zuOLbdqFPX6THpJYnnzZfpd75B2IVynY4cJSLfAlJouEQORA65B5076qx
2MpmT0E5itVcqZoKuIrVnOcWPnO7ZY0BJ3RxVJZcNPNDCzsZxGCJ14UM7J616Lz5
jparl7cj4+YNNu+RwnkO+Nys6om4Txcpe32VfUmTG5qdHNqCm15oTisw3SeCf0yg
IsxX6pagbMj+32WJKWJHqW4uftmuvljfa6tUfyfaqHj2uHYdXX+Yy0YFKkLSnVG
PiY9Dwo5Hlu+NutnsSCYU4bPJlgwE3lzMgOwRjCwBRay+DdL2kGFnK0tqwGRPd08
+MhCyNHgiE5Va7GX4USmf+0J6nsQ/yUfPL9UMo2Jp0vypmaw2Q9iKwKfVPE2HIDB
BP4slhwC4yjbricp7+Jx3+cGTxqdyvAaBl2xzlzY+EW2YpD7zu+K/OPm/2etcZD
IuCJsSUxGShCIJKIDhV8DijPk+zxu2b1taVuAEidFWH6kmPSgnQIQ2g3VJdK7+a9
kVzupLcRdQYsRn3C1habZiYIIUmO8CUJnGXfEsqHKE2j2oTAt197gb90Pn5aHo1F
yu/50+XH9sIP4ICOYjM0TqP/csnWyQVsbv7wmT7TUO41P1c4MZvkW7/XxAmO9Nq
i12VCJslY4SFka8rVWbhbC2zT//He+KKKgV14wm87C510hx2bq3WmDcE0C/oqAnf
ykeS8j3afBCiu67A1c6YNaEqGU+aqGaL2OeCW9znNur0XWqpoP2Djghm8c53I/x
bNDNqsg7+S6jSx8Qhm6sfKTQEXja5dq6rU7xDSASp49ifPsoVIFEIINuuWxwuB
EUEra/bXhtAvWnvqzdxMfnml4smRA0KJpl39S0glukHipyRm1Bh6byDn10lq/D4
b7meo39rFBQTxM9YW2sm0qClIFED3Hkr9NrP(U0u27YMDrpMnx01qrJp3dghsz
R0McFow2WaZsX6gmqUfWgmOHzkD/2YK5S5Ax9r2VuGeXXyBhAjNr64BVHH1wLoOU
AssK86kgaw19mjd2Gh/5nmSmuqDGNwWK5edT4NGZcr4vA0PwU+mHZIax9y5FOWX
7rrIX8zQbuFqSgFtmctwIPdwyrobw6mA9sZUS7ncs+Sv8hhHD2Mi2XXtXJtqmyMJ
TMGSL/AAXuq76YgRSIDTZAHXenvyzLF2OUWpsqd3chVj0gCbWIX5FVHRkN40x5
ImK9FhxHjGuWAX/ix7zQ3+zvIZZPFTkbVzK4xijFdCkWgK0006oFeOas3/hkAHS7
6BX3JdFymaTQsowgaeQ+cSiUlogTWymKSYPyN6XSbHRR3G6vw/272akU04es2PMi
GgFKML/8Dh51UNYpbM/ImUdzK/94iqIvdAFBE81Hg98CXcRQUCIh2JohOb0/pLa
qVfVZzi3aVtGmpJYqdH1Uq8Qq1KKr+7c+MURb1Sjsaal1J7XQZ0RbiBxSUUKnxb
f011RaX+JvYq+gVlloC1h+1Wai2sE6muCTw8aEGG2FFliRihz2JMESjptuxHyVPQ
THQIMnqSE/H0yteNR6rs50pW0vXBhFTaFd/DQAnT7/N8/d3Raq2OkeSt7eOHkucC
ZALThljUc3EKmdyjX7RP0vEZIqGiO3XTzpQtaNewCa7vcEe4HkIvpRsHvEBfmFa
0xDN3bSXyziLUBgeieonfcmvrQc6kHEuDTZs1oCKfulaXHIEGC/kopvfiJX8QTPJ
1RsVDXEOLcaOzX5M6j5Z+w+mnFvdDQ37YFoWUbP02d/CwpUwbTLVSQXhTE9LGIH
RfArioSyO/ouwt6S2ag+XH2yprFRoumbQ8IAgomD5m1XF1ek9FLWE2s2oYN34goX
iGwaYeu9vyUBUtxrakVRfMiLkpnome7aeA0cBy2TAECD4rdzxYhmLTGfnDizE274
Asxv2SgZSG2FkKaH4Q5Phm6mEGGGV7NDpB6CGYx8pHWJdBKTKeweZuHO1zyck7w
/fPrpdNP/FriE5GiTKM/dzBHJXmoV7zrbXanFMmR+NYthijjGveGmp4DTP5Pp1C9
dKbdKySBI/CvFi2JxL880zWNCBm9cUNbTpYYAW/5Ht4dFzuO/83a8yfD33uvqyd1
5Z4glOOhUf8OhvbP9baLAgFi2gRHB7F37M5DR2rL0E1NhuW7uXZ0VIGxT/NiW75
9SFkH8DCGQIEXjd01j7hE1SgGdP2DRYXXU75YEOhur3Pu+6BUS0pFx9D90OdWjKe
Lu488J4yVfXblloX4/O/OmFKKdL8DraRIsKOAeAAGL2UYmfLsl/yWbWQHnv
lmO55Zb+RKEY1KASbiABrGZcOo1Yr2I8AIdwtNvQ6WH95zrsQzDy2M2ZBnjDD92
AyyvR13A4LFdiqbXuiBlqgrhdFUHuZfQFHDhNpWzYvfk8L6h9c1B5rnuY271V
mp3aqOlbRu5s0xaaxTzfYrss018dhOon5YN0GHJtNNBmN5EFPgkCqM2mRqhLQ4UQ
ESV95QXhbH9aaEggs+VvnMNQEKsU1v3x6N7c+Sf3+yelhLXFgimtUiZisuQavssNn
ljpL
=2Nfc
-----END PGP MESSAGE-----

=====
===== End Part 2 =====
=====

190

DUMP ROM 2000 ST16

2000 0d 04 2a 3f 00 8e 20 fb 9d 33 25 80 80 00 d6 e0
2010 00 81 0f 00 01 0f c8 cc ae 0a d6 20 0d e7 29 5a
2020 2a f8 81 ad f3 cd 21 41 cd 20 e8 20 fe 06 02 09
2030 02 00 f0 0e 04 ed cc 1e af 1e 04 cc 22 1a 0c 04
2040 03 07 01 03 cc 40 1e ad cf 0f 04 03 cc 22 37 06
2050 02 e7 cc 1f 28 3f 27 3f 28 3f 29 ad 75 be 2f b6
2060 2e bb 2b b7 2b 5a bd 2a bb 27 b7 27 24 06 3c 28
2070 26 02 3c 29 5d 26 ee 3a 2b 3a 2e 2a e8 ae 02 e6
2080 27 cd 22 b3 5a 2a f8 4f 81 12 04 b6 01 13 04 3f
2090 01 ad 49 a6 40 ad 45 16 02 14 04 20 fe b6 2e a1
20a0 10 26 37 4f 04 21 07 cd 22 f6 bd 2a ba 25 e7 36
20b0 5c b3 2e 26 ee ad 51 ad 17 bd 2a e1 36 26 1b 5c
20c0 b3 2e 26 f5 4f 20 15 cd 1f 55 ad 1c ad 6e 20 85
20d0 ad 45 3f 03 01 21 02 16 03 81 a6 fa 0e 04 04 cd
20e0 1f 77 4f b7 20 81 a6 ff 10 2b ad 0f 1a 03 ad 27
20f0 11 2b b6 30 27 02 ad 35 3f 03 81 5f 4d 26 02 14
2100 21 e7 36 5c a3 20 26 f9 ad 4d 5a 3c 2a e6 36 bd
2110 2a 5a 2a f9 3a 2a 81 17 03 18 03 04 21 04 10 03
2120 20 02 14 03 07 01 04 3f 03 20 fe b6 31 ae 63 5a
2130 26 fd 4a 26 f8 11 03 15 03 15 21 81 ae 06 cc 20
2140 1a 18 01 ad 12 10 03 14 03 1c 03 4f c7 e1 00 11
2150 03 18 03 a6 1e 20 9f 12 03 13 03 81 99 39 88 ad
2160 f6 ae 1f e6 80 d7 e0 00 5a 2a f8 cd 20 d0 ae 1f
2170 d6 e0 00 e1 80 27 02 10 20 6f 80 5a 2a f2 81 ad
2180 bb a6 20 b7 2c a6 e0 b7 2f 81 ae 1f d6 e0 00 e7
2190 80 5a 2a f8 81 12 04 20 10 5f ad bb a6 ff d7 e0
21a0 08 5c a3 08 26 f8 cd 21 17 4f c7 df fe b7 27 18
21b0 03 10 03 ad 14 10 04 ad 12 11 04 4c ad 0d 4c 3a
21c0 27 26 f2 3f 03 3f 04 3f 01 a6 0a ae 63 5a 26 fd
21d0 4a 26 f8 81 10 02 cc 22 b9 ad f9 ad bc 3f 20 20
21e0 69 cd 26 18 20 fb 20 55 23 88 1f c7 1f a7 1e 4f
21f0 20 c7 1f b3 1f b1 1e 08 1e 4a 1f ce 24 4a 24 6a
2200 21 41 21 95 24 1c 1e 8a 21 d4 24 1b 24 28 20 89
2210 1f 9b 25 13 21 d9 21 e1 23 96 c6 e0 08 27 fe 43
2220 27 fe cd 22 ea c6 e0 09 27 fe 43 27 fe a6 3b cd
2230 22 b9 3f 01 cc 24 6e a6 1e b7 31 a6 0b ad 7a 5f
2240 d6 e0 00 ad 74 5c a3 09 26 f6 a6 90 ad 6b b6 20
2250 ad 67 4d 26 fe 5f cd 22 fc e7 56 5c a3 05 26 f6
2260 b7 2e b6 56 a1 88 27 0c a6 6e 20 02 a6 6d 20 dc
2270 a6 6b 20 d8 be 57 56 25 f3 5a a3 0a 24 ee b6 26
2280 a1 79 27 04 a3 03 26 e4 b6 2e a1 11 24 e2 4d 27
2290 df b6 58 a4 ef b7 2b a1 e0 25 d5 26 06 b6 59 a1
22a0 10 25 cd b6 57 ad 12 b6 59 a4 f0 b7 2c 58 dd 23
22b0 5f 20 97 0e 04 03 cc 1f 77 bf 24 b7 25 ad 2b 11
22c0 00 ae 08 bf 22 3f 23 9d ad 20 46 25 04 11 00 20
22d0 04 10 00 33 23 3a 22 26 ef ad 0f 00 23 04 11 00
22e0 20 02 10 00 ad 04 10 00 b6 25 ae 43 5a 26 fd be
22f0 24 81 ae 22 20 f6 0e 04 03 cc 1f 55 bf 24 00 00
2300 fd 3f 23 ad ed 00 00 f6 ae 08 bf 22 ad dc 01 00
2310 14 31 23 20 03 9d 20 fb 46 3a 22 26 ef b7 25 ae
2320 1d 20 c9 cc 21 99 cd 21 7f a6 7f b7 27 3c 2a ae
2330 1f cd 21 57 a6 ff bd 2a 5a 2a fb cd 21 17 cd 23
2340 dc 3a 27 26 ea 3a 2a 10 21 cd 21 7f cc 20 55 ad
2350 fd cd 21 8a 11 21 cd 21 3c cd 20 ca cc 21 5c 20
2360 e8 20 c3 20 ea 20 0c 20 1b 20 31 20 b6 20 19 20
2370 37 20 78 a6 79 b7 26 ad 83 d1 e0 09 27 02 3f 26
2380 5a 2a f4 81 5f cc 20 9d a6 40 ae 3f b7 2b 3f 2c
2390 bf 2e 3f 2f 20 b6 a6 28 ae 0b 20 f0 cd 21 8a a6
23a0 ff 10 21 cd 20 ca 20 ac ad 06 9c ae 06 cc 22 40
23b0 ad 4e ca e0 07 b1 f5 26 fe cd 21 57 c7 e0 07 b6
23c0 01 a4 d7 26 fe 18 03 10 03 a6 1e cd 20 f6 ad 30
23d0 c1 e0 07 26 fe 81 cd 20 fb cd 21 17 a6 20 bb 2c

EXHIBIT 2

2400 ae 06 3f f5 bf f6 d6 e0 00 ae 08 46 25 02 3c f5
2410 5a 26 f8 be f6 5a 2a ec b6 f5 81 8e ad 0e 83 b6
2420 25 ad 02 bd 80 cc 20 dc ad 02 bc 8a ae 12 d6 24
2430 37 e7 80 5a 2a f8 81 ae 08 1e 01 8e 3f 01 cc 1f
2440 66 16 02 c6 20 00 17 02 4f 81 cd 20 e6 16 02 ad
2450 85 4f ad 82 17 02 3f 2c ad 03 cd 23 dc ae 1f bd
2460 2a 43 26 03 5a 2a f8 cc 20 dc b6 21 b7 03 5f 4f
2470 e7 20 d7 01 00 5c 26 f8 ae 20 f6 26 55 73 73 73
2480 5c 26 f7 d6 01 00 26 37 43 d7 01 00 4f d7 01 00
2490 43 d7 01 00 5c 26 ec ae 20 f6 43 26 35 f7 f6 26
24a0 31 73 5c 26 f4 d6 01 00 43 26 14 d7 01 00 d6 01
24b0 00 26 0c 43 d7 01 00 5c 26 eb 5a d6 01 00 43 26
24c0 42 d7 01 00 43 d7 01 00 4f d7 01 00 5d 26 eb 5a
24d0 f6 43 26 35 73 73 73 a3 20 26 f4 5f 5a d6 01 00
24e0 26 21 43 d7 01 00 d6 01 00 43 26 17 d7 01 00 5d
24f0 26 ea 5a f6 26 13 73 f6 43 26 0e f7 a3 20 26 f2
2500 5f 20 0a a6 01 b7 20 20 02 3f 20 1e 20 bf 36 9c
2510 cc 20 3e 3f f6 3f f7 3f fa ad 21 3c fa ad 3c 3c
2520 fa ad 4f 3c fa ca 26 02 3c fa cd 26 18 06 01 0a
2530 b6 f6 cd 22 b3 b6 f7 cd 22 b3 4f 81 a6 50 b7 fe
2540 a6 40 ae 0c ad 0d a6 e0 ad 02 a6 40 f7 f1 27 02
2550 10 f6 81 ad f7 4c b1 fe 26 f9 81 cd 26 13 ae 0d
2560 4f ad f0 a6 08 ad e5 a6 80 ad e1 a6 20 ad dd 4f
2570 20 da a6 3f b7 fb ad 1a ad 1c 3c fa 1e 0d 34 fb
2580 ad 10 3c fa a6 44 ae 04 b1 0e 27 02 1a f6 5a 26
2590 f7 81 a6 01 b7 ff ad 00 b6 fb b7 fe 4f ae 43 ad
25a0 11 ae 41 ad 0d ad 6c ae 45 ad 07 ae 46 ad 03 38
25b0 ff 81 02 ff 16 04 ff 24 06 ff 34 bf 0c b7 0b b1
25c0 0b 27 02 12 f6 4c b5 fe 26 f3 81 bf 0c 16 0c 9d
25d0 b1 0a 27 02 14 f6 4c b5 fe 26 f5 81 bf 0c ae 55
25e0 bf 0b b3 0b 27 02 16 f6 53 4c b5 fe 26 f2 81 bf
25f0 0c 16 0c ae 55 b3 0a 27 02 18 f6 53 4c b5 fe 26
2600 f4 81 04 f6 0d a6 40 ae 6d ad c0 04 f6 02 1c f6
2610 15 f6 81 ae 03 bf fe 81 ad f9 a6 06 ae 80 ad 65
2620 a6 3f b7 f9 3f f8 ad 29 37 f9 a6 80 b7 f8 ad 21
2630 1d 0c a6 60 97 ab 1f b7 fe b6 0a d1 27 73 27 02
2640 10 f7 5c b3 fe 26 f2 b6 0e d1 27 73 27 02 14 f7
2650 81 ad 40 3c fa a6 4d b7 fc a6 07 b7 fd a6 01 ba
2660 f8 37 fc 25 06 b7 0d ad 39 20 06 aa 02 b7 0d ad
2670 35 3a fd 26 e8 a6 49 b7 0c b6 f8 44 97 bb f9 b7
2680 fe 3c fa 20 b4 b7 0c d6 26 ef b7 0b 5c 9f b5 fe
2690 26 f5 81 a6 02 ba f8 b7 0d b6 f9 b7 fe a6 02 5f
26a0 ad e3 18 0c 20 3a cd 26 13 a6 45 ae 40 ad d6 a6
26b0 07 0e 0d 02 a6 0f b7 fb 18 0c 4f 08 0d 06 4a 26
26c0 fa 12 f7 81 d6 26 ef b7 0b 5c d6 26 ef b7 0b 5c
26d0 d6 26 ef b7 0b 5c d6 26 ef b7 0b 5c 3a fb 26 da
26e0 a6 1e 5f 0c 0d 08 5a 26 fa 4a 26 f6 1e f6 81 11
26f0 32 54 76 98 ba dc fe 10 32 54 76 98 ba dc fe 10
2700 32 54 76 98 ba dc fe 10 32 54 76 98 ba dc fe 10
2710 32 54 76 98 ba dc fe 10 32 54 76 98 ba dc fe 10
2720 cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 ef
2730 cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 71 ef
2740 cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 01 ef
2750 cd ab 89 67 45 23 01 ef cd ab 89 67 45 23 81 0f
2760 01 ef 0f d2 45 2a 49 80 9d 02 35 28 7c 92 cd 94
2770 70 f8 5b 57 d9 53 3b 14 d7 8b c8 62 49 5f e6 eb
2780 69 cb 16 fa 3a ac 5f 81 14 df 07 c7 de 7a d1 57
2790 0e a0 b4 09 1e a4 27 3a 78 c5 4c 78 4f b2 ee c0
27a0 38 e2 ba ae f6 32 4f 64 f3 9b af c4 f9 e4 13 92
27b0 4f 0e ad 2a 51 2c 24 e8 aa 47 55 a1 ad c8 87 40
27c0 ea ef 22 bf 28 87 c5 fc ad 78 ae d5 2b 39 8a 2a
27d0 0a eb ab 3b 83 80 9a 80 65 24 54 b2 df 1c fe d8
27e0 a4 cc 21 ff ff ff ff ff ff ff ff ff ff ff ff

2820 40 cd 29 cf cd 29 c8 18 0c 0c 0d 06 5a 26 fa 4a
2830 26 f7 a6 09 b7 0c a6 67 b1 0a 26 05 a0 22 24 f8
2840 4f 3f 0c 3f 0d 81 b6 0c a4 87 b7 0c 81 b6 0c a4
2850 87 aa 60 20 f5 b6 0c aa 40 20 ed b7 0c a6 04 b7
2860 f5 81 a6 06 ad f5 20 19 a6 0e ad ef 20 4b 3f f5
2870 a6 43 20 04 3f f5 a6 01 3d f5 26 03 cd 29 1b b7
2880 0c cd 29 e1 0e f5 03 4f 20 05 b6 f5 a4 7f 4a 97
2890 0e f5 0a bd f1 b7 0b 5c b3 f5 26 f7 81 bd f1 b7
28a0 0b 5a a3 ff 26 f7 81 3f f5 a6 4b 20 04 3f f5 a6
28b0 49 3d f5 26 02 ad 64 b7 0c 3a f5 b6 f5 a4 7f 27
28c0 2c cd 29 e1 3c f1 0e f5 03 4f 20 04 b6 f5 a4 7f
28d0 97 0e f5 0b b6 0a bd f1 5c b3 f5 26 f7 20 07 b6
28e0 0a bd f1 5a 26 f9 b6 0e bd f1 3a f1 81 b6 0e 81
28f0 ae 40 a6 01 20 02 a6 43 b7 0c 9f ab 40 0f 0d 02
2900 a0 20 b7 f5 20 08 a6 43 20 02 a6 01 ad 0b d6 01
2910 00 b7 0b 5c b3 f5 26 f6 81 b7 0c ae 40 0f 0d 01
2920 54 bf f5 5f 81 ae 40 a6 49 20 02 a6 4b b7 0c 9f
2930 ab 3f 0f 0d 02 a0 20 b7 f5 20 06 a6 49 ad da 3a
2940 f5 b6 0a d7 01 00 5c b3 f5 26 f6 b6 0e d7 01 00
2950 81 cd 28 6e 5f a6 46 b7 0c cd 29 e1 bd f1 b7 0b
2960 5c a3 04 26 f7 20 08 5f a6 46 b7 0c cd 29 ea 16
2970 0c a6 20 b7 f5 ae 08 6f f5 5a 26 fb 3c fd 01 fd
2980 00 36 f6 36 f7 36 f8 36 f9 01 fd 18 b6 0a bb fd
2990 b7 fd b6 0a b9 fc b7 fc b6 0a b9 fb b7 fb b6 0a
29a0 b9 fa b7 fa 36 fa 36 fb 36 fc 36 fd 3a f5 26 ce
29b0 17 0c ae 04 e6 f5 b7 0b 5a 26 f9 81 a6 46 b7 0c
29c0 a6 01 b7 0b ae 03 20 06 a6 46 b7 0c ae 04 4f b7
29d0 0b 5a 26 fb 81 a6 40 20 02 a6 60 b7 f3 a6 01 b7
29e0 f2 a6 d6 b7 f1 a6 81 b7 f4 81 d6 01 00 b7 0b 5c
29f0 d6 01 00 b7 0b 5c d6 01 00 b7 0b 5c d6 01 00 b7
2a00 0b 5c 81 a6 01 20 05 cd 28 46 a6 02 ad 32 18 0c
2a10 0d 0d fd 81 be f6 20 01 5f ad 06 ad 15 0d 0d fd
2a20 81 a6 03 ad 1b a6 45 b7 0c a6 0f 0f 0d 01 44 b7
2a30 f5 81 ad b6 18 0c 09 0d fd ad af 3a f5 26 f7 81
2a40 b7 f5 b6 0d a4 f0 ba f5 b7 0d 81 be f6 ad b8 ad
2a50 c8 20 c6 be f6 ad b0 ad c0 9f a0 20 0e 0d 02 a0
2a60 20 97 20 ed bf f6 a6 23 b7 0d 1d 0c 5f ad 6c cd
2a70 29 bc be f6 a6 07 b7 f5 a6 45 b7 0c ad b4 09 0d
2a80 fd ae 04 cd 29 ce 0d 0d fd 1b 0d 81 ad 0a be f6
2a90 20 bd ad 04 be f6 20 bf a6 4b cd 29 19 3a f5 98
2aa0 5c 4f b2 0a e7 ff 3a f5 26 f6 4f b2 0e d7 01 00
2ab0 cd 29 0a a6 49 cd 29 19 3a f5 98 5c b6 0a 49 e7
2ac0 ff 3a f5 26 f6 b6 0e 49 d7 01 00 cd 2a 18 ae 09
2ad0 0f 0d 01 5a cd 2a 03 5a 26 fa 81 a6 01 b7 0c a6
2ae0 20 b7 f5 cd 28 81 ae 20 cc 29 ce be f6 cd 28 f2
2af0 cd 29 3b ae 40 cd 29 2b ae 42 cd 2d f4 cd 29 d5
2b00 3f f8 be ff d6 01 3f 26 02 3a ff ad 64 ad 46 20
2b10 44 cd 29 1b b6 06 5c e7 ff 26 02 3c 06 b3 f5 26
2b20 f3 81 ad ed c6 01 00 aa 01 c7 01 00 cd 29 06 cd
2b30 29 67 ad dd cd 29 0a ad d8 cd 2a 18 cd 2a 03 cc
2b40 29 3b be f6 4f b7 f8 cd 2a 07 cd 2a 19 cd 29 3b
2b50 8f ad 1e 27 1b a6 03 cd 2a 40 a6 01 b7 0b ae 03
2b60 cd 29 ce 18 0c 09 0d fd ae 04 cd 29 ce 0d 0d fd
2b70 81 be ff 27 55 5a bf ff cd 29 e1 bd f1 27 4b b7
2b80 f6 a6 08 b7 f7 cd 2a 21 3a f7 39 f6 24 fa 3d f7
2b90 27 25 13 0d 18 0c 0d 0d fd 06 f8 06 39 f6 24 13
2ba0 27 06 39 f6 25 02 16 0d 12 0d cd 2a 25 5f cd 2a
2bb0 1b 17 0d 3a f7 26 db be ff 27 0d 5a bf ff a6 08
2bc0 b7 f7 bd f1 b7 f6 20 ca a6 55 81 cd 23 f1 cd 29
2bd0 e1 cd 2c 65 cd 29 25 cd 2c c1 cd 2c 65 cd 29 3b
2be0 ed 2c 91 ae 20 cd 29 27 a6 80 cd 2c cf cd 29 51
2bf0 cd 28 10 cd 29 3b cd 2c 91 cd 29 3b a6 60 cd 2c
2c00 cf ad 59 5c e6 ff d2 01 1f e7 ff 3a f5 26 f4 24
2c10 0f ad 49 bd f1 5c e9 ff e7 ff 3a f6 26 f5 24 f1

2c40 49 b7 0c ad 17 b6 0a 5c d9 01 1f e7 ff 3a f5 26
2c50 f4 4f b9 0a 5c e7 ff 3a f6 26 f6 81 a6 20 b7 f6
2c60 b7 f5 5f 98 81 3f 0d ad 43 ad 45 1e 0d cd 29 51
2c70 1f 0d ad 0f cd 2a 07 ad 06 cd 2a 18 1e 0d 81 a6
2c80 49 20 02 a6 4b b7 0c ae 1f b6 0a 5a 26 fb 17 0c
2c90 81 cd 2c b9 ae 1f ad 08 3f f8 cd 2b 71 cc 2b 55
2ca0 bd f1 4d 26 03 5a 20 f8 5c bf ff 81 a6 43 20 02
2cb0 a6 01 b7 0c ae 40 cc 29 ce a6 60 20 06 a6 40 20
2cc0 02 a6 20 bb f3 b7 f3 4f b9 f2 b7 f2 81 a6 20 97
2cd0 b6 f3 bf f3 b0 f3 b7 f3 b6 f2 a2 00 b7 f2 81 cd
2ce0 23 f1 3f 0d cd 28 74 cd 29 3b ae 20 cd 2a 64 cc
2cf0 29 3b be f6 cd 2a 07 cd 2a 19 a6 10 b7 f6 cd 2a
2d00 03 3a f6 26 f9 cc 2a 59 3f 0d cd 29 51 ad ae ae
2d10 3f ad 8d 5f cc 2b 44 cd 23 f1 ae 60 bf fe cd 2e
2d20 9f ad 51 ae 80 bf fe cd 2e 9f ad 48 cd 29 d9 cd
2d30 29 51 ae 62 cd 2d f4 a6 20 b7 ff ae 80 cd 2b 44
2d40 ae a0 cd 29 27 ae 60 cd 29 2b cd 29 d9 cd 2c e2
2d50 cd 29 06 cd 29 67 ae 40 a6 55 e7 ff 5a 26 fb cd
2d60 2c f4 cd 29 3b cd 2b ce ae 40 e6 ff a1 55 26 aa
2d70 5a 26 f7 81 cd 2e 40 ad 42 cd 2d e4 a6 23 b7 0d
2d80 be fe cd 2e 2f a6 01 b7 0c 3f 0b 9f ab 20 b7 f5
2d90 3f 0b cd 29 0e ae 1e cd 29 ce cd 2e 04 cd 2e 6a
2da0 cd 2a 0e be fe cd 2e 39 9f ab 60 97 a6 83 b7 0d
2db0 cd 29 27 b6 fe ab 60 97 cc 2e 39 cd 29 3b c6 01
2dc0 00 c7 01 a0 c6 01 01 c7 01 a1 a6 45 b7 0c a6 0f
2dd0 b7 f5 13 0d cd 2a 0e 12 0d cd 2e 5c cd 2e 87 3a
2de0 f5 26 ef 81 a6 49 b7 0c 9d b6 0a c7 01 a0 b6 0a
2df0 c7 01 a1 81 e6 fe a0 02 e7 fe e6 ff a2 00 e7 ff
2e00 5c 25 f7 81 cd 29 c8 a6 23 b7 0d a6 45 b7 0c ae
2e10 04 cd 29 ce ae 0f 18 0c 09 0d fd b7 0b 5a 26 f8
2e20 c6 01 a0 b7 0b c6 01 a1 b7 0b 0d 0d fd 81 5f d6
2e30 01 00 a4 fe d7 01 00 81 5f d6 01 00 aa 01 20 f4
2e40 a6 83 b7 0d ad 20 ad 2e a6 01 b7 0c a6 01 b0 f5
2e50 b7 0b 4f b2 f6 b7 0b ae 1e cc 29 ce c6 01 a0 b7
2e60 0b c6 01 a1 20 0c a6 46 20 02 a6 45 b7 0c a6 ff
2e70 b7 0b ae 02 20 0c a6 43 b7 0c a6 01 b7 0b 3f 0b
2e80 ae 1d b7 0b cc 29 ce b6 0d a4 f0 aa 03 b7 0d 18
2e90 0c 09 0d fd ae 04 3f 0b 5a 26 fb 0d 0d fd 81 1e
2ea0 0d cd 2b 22 ad 92 c6 01 1f aa c0 c7 01 1f cd 2f
2eb0 82 4f 3f f5 cd 2f ef cd 29 06 cd 29 67 ad 11 27
2ec0 04 a6 02 20 ed 81 03 05 07 0b 0d 11 13 17 1d 1f
2ed0 a6 0a b7 f6 a6 01 b7 0c be f6 d6 2e c5 b7 0b ae
2ee0 1f cd 29 ce ad 55 a6 49 b7 0c be f6 b6 0a d1 2e
2ef0 c5 26 d2 ae 1e 3d 0a 26 cc 5a 26 f9 3d 0e 26 c5
2f00 3a f6 26 d0 be fe cd 29 2b a6 83 b7 0d cd 2e 2e
2f10 cd 2e 66 cd 2e 76 a6 01 cd 2f d0 cd 2a 18 a6 49
2f20 b7 0c 9d b6 0a b7 f5 b6 0a b7 f6 cd 2e 38 3d f5
2f30 26 07 3d f6 26 03 ae 01 81 5f 81 a6 05 b7 0c ae
2f40 20 bf ff c6 01 1f 49 b7 f5 a6 07 b7 f7 a6 81 b7
2f50 0d 18 0c 0d 0d fd 39 f5 24 13 a6 83 b7 0d be f6
2f60 d6 2e c5 b7 0b ae 03 cd 29 ce cd 2e 87 3a f7 26
2f70 d6 3a ff 27 0c a6 08 b7 f7 be ff e6 ff b7 f5 20
2f80 d6 81 4f c7 01 21 c7 01 22 c7 01 23 a6 01 ad 40
2f90 a6 03 ad 21 b7 f4 a6 01 ad 36 a6 05 ad 17 b7 f3
2fa0 d6 02 ad 2c a6 07 ad 0d b7 f2 a6 09 ad 22 a6 0b
2fb0 ad 03 b7 f1 81 c7 01 20 ad 10 ae 20 cd 29 68 cd
2fc0 d6 18 a6 49 b7 0c 9d b6 0a 81 b7 f5 a6 43 20 04
2fd0 d7 f5 a6 01 b7 0c b6 f5 b7 0b ae 1f cc 29 ce b7
2fe0 f6 5a e6 f1 b1 f6 25 02 b0 f6 e7 f1 81 a6 02 4d
2ff0 27 0d 3c f5 3c f5 ae 04 6c f0 6c f0 5a 26 f9 ae
3000 04 a6 03 ad da a6 05 ad d6 a6 07 ad d2 a6 0b ad
3010 ce ae 04 fd f0 27 d6 5a 26 f9 b6 f5 cb 01 00 c7
3020 01 00 ae 02 24 08 4f e9 ff e7 ff 5c 20 f6 81 cc
3030 28 46 1f 0d 81 1e 0d 81 cc 28 4d cc 28 55 cc 28

194

3000 2a 07 cc 2a 14 9d 5 81 cc 2a 03 cc 2a 4b cc 2a
3070 53 cc 2a 66 cc 2a eb cc 2b 22 9d 9d 81 cc 2b 42
3180 cc 2b 42 9d 9d 81 cc 2d 17 cc 2d 08 cc 2b cb cc
3090 2c f2 cc 30 a4 cc 32 56 cc 2c df cc 2a 98 cc 2a
30a0 8c cc 2a 92 cd 23 f1 3f 0d cd 29 e1 cd 31 5a ae
30b0 60 cd 29 27 a6 30 cd 2c c3 cd 31 5a cd 29 3b a6
30c0 90 cd 2c c3 ae 2f cd 2c a0 cd 2b 50 ae c0 cd 29
30d0 27 a6 c0 cd 2c cf cd 29 51 cd 32 38 a6 90 cd 2c
30e0 c3 ae 2f cd 2c a0 ae 60 cd 28 f2 cd 32 25 cd 29
30f0 3b cd 2b 50 cd 29 3b a6 90 cd 2c cf cd 31 df 5c
3100 e6 ff d2 01 bf e7 ff 3a f5 26 f4 24 10 cd 31 df
3110 bd f1 5c e9 ff e7 ff 3a f6 26 f5 24 f0 cd 2c b9
3120 cd 28 74 cd 32 25 5f cd 31 e4 cd 29 3b 3f ff ae
3130 2f ad 6c cd 29 3b a6 30 cd 2c cf cd 31 f1 cd 31
3140 df 5c e6 ff d9 01 bf e7 ff 3a f5 26 f4 24 0a ae
3150 31 4f e9 ff e7 ff 5c 25 f8 81 1d 0c cd 29 51 cd
3160 32 38 cd 32 4d cd 2a 07 cd 32 43 cd 32 49 ae 30
3170 ad 72 ae 90 bf ff a6 49 b7 0c ad 63 5c b6 0a e9
3180 ff d7 01 8f 3a f6 26 f4 24 13 98 5f bd f1 b7 f6
3190 d6 01 90 b2 f6 d7 01 90 5c 3a f5 26 ef ae 3e cd
31a0 32 4f cd 2a 07 cd 32 43 cd 32 49 cd 2a 03 a6 03
31b0 b7 0d a6 45 b7 0c ae 04 cd 29 ce ae 08 18 0c 09
31c0 0d fd 3f 0b 5a 26 f8 a6 01 b7 0b ae 03 cd 29 ce
31d0 09 0d fd ae 04 cd 29 ce 0d 0d fd be ff 20 05 a6
31e0 30 cc 2c 5e cd 2a 21 a6 0c b7 f5 cd 2a 32 cc 2e
31f0 94 a6 23 b7 0d 1d 0c cd 29 c8 cd 28 74 ad 26 cd
3200 2a 18 cd 29 25 cd 28 74 ad 1b cd 29 bc cd 2a 18
3210 a6 49 b7 0c a6 40 ad c9 b6 0a 5c d2 01 3f e7 ff
3220 3a f5 26 f4 81 a6 49 ae 2f ad 11 ae 0f a6 4b b7
3230 0c 9d b6 0a 5a 26 fb 81 ae 2f a6 4b ad 13 ae 10
3240 cc 29 ce a6 01 b7 0c 20 f5 a6 43 20 f8 ae 2f a6
3250 4b ad dc 17 0c 81 cd 23 f1 cd 29 e1 b6 f2 b7 fb
3260 b6 f3 b7 fc b6 fd b7 f2 b6 fe b7 f3 5f bd f1 d7
3270 01 a0 5c a3 60 26 f6 a6 23 b7 0d 1d 0c cd 29 c8
3280 b6 fc ab 80 b7 fa 4f b9 fb b7 f9 ad 27 a6 10 b7
3290 f7 a6 01 b7 f9 a6 a0 b7 fa ad 19 3a f7 26 f2 b6
32a0 fd b7 f9 b6 fe b7 fa ad 0b ae 60 d6 01 9f e7 ff
32b0 5a 26 f8 81 ae 70 6f ff 5a 26 fb a6 a0 ad 35 a6
32c0 c0 ad 31 a6 e0 ad 2d cd 33 d7 a6 60 cd 31 e1 bd
32d0 f1 b7 f5 d6 01 00 b2 f5 d7 01 a0 5c 3a f6 26 ef
32e0 24 11 d6 01 00 a2 00 24 0a ae 60 e6 ff d7 01 9f
32f0 5a 26 f8 81 b7 f8 cd 33 bf cd 33 95 be f8 ad 63
3300 5f cd 33 a0 cd 33 ec cd 33 95 5f ad 56 cd 33 88
3310 cd 33 d7 cd 33 95 ae 80 ad 49 5f cd 33 a0 5f 5c
3320 d6 01 1f e7 ff a3 50 26 f6 ae 20 4f d7 01 4f 5a
3330 26 fa cd 33 e0 ad 5e ae 80 ad 28 5f ad 62 cd 33
3340 e6 ad 52 ae 80 ad 1c ae 20 ad 55 cd 33 cb ad 45
3350 be f8 ad 0f 5f ad 49 ad 78 ad 3a be f8 ad 04 ae
3360 20 20 3d a6 45 b7 0c a6 04 3f 0b 4a 26 fb a6 08
3370 b7 f5 b7 f6 a6 15 b7 0c 09 0d fd 3f 0b 3a f6 26
3380 f7 cd 2a 39 0d 0d fd 81 a6 49 b7 0c a6 9f b7 f5
3390 ae 80 cd 29 41 cd 2c b0 ae 20 bf f5 5f cc 28 81
3400 a6 49 b7 0c a6 40 b7 f5 98 b6 0a 5c e9 ff e7 ff
3410 3a f5 26 f5 24 08 4f 5c e9 ff e7 ff 25 f8 81 b6
3420 fa 98 b7 f3 b6 f9 a9 00 b7 f2 81 b6 fa ab 20 20
3430 f1 b6 fa ab 40 20 eb b6 fc 98 b7 f3 b6 fb 20 e6
3440 b6 fc ab 20 20 f4 b6 fc ab 40 20 ee b6 fc ab 60
3450 00 c0 ff ff ff ff ff ff ff ff ff ff ff ff ff
3460 ff bf ff ff ff ff ff ff ff ff ff ff ff ff ff
3470 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3480 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3490 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3500 00 00 00 00 00 00 00 00 00 00 00 00 00 00

ST16CF54

DATA SHEET

DS.CF54/9601V1

INDUSTRY DISTRIBUTION- NDA submitted- Do NOT copy without written authorization from
SMARTCARD Div. Marketing Dpt. Rousset

1 SQUIRE, SANDERS & DEMPSEY L.L.P.
P. Craig Cardon (State Bar No. 168686)
2 Michael T. Purleski (State Bar No. 216307)
801 S. Figueroa St., Fourteenth Floor
3 Los Angeles, California 90017
Telephone: (213) 624-2500
4 Facsimile: (213) 623-4581

5 T. WADE WELCH & ASSOCIATES
T. Wade Welch (*pro hac vice*)
6 Ross W. Wooten (*pro hac vice*)
Joseph H. Boyle (*pro hac vice*)
7 2401 Fountainview Suite 700
Houston, Texas 77057
8 Telephone: (713) 952-4334
Facsimile: (713) 952-4994

9 Attorneys for Plaintiffs
10 ECHOSTAR SATELLITE
CORPORATION,
11 ECHOSTAR COMMUNICATIONS
CORPORATION, ECHOSTAR
12 TECHNOLOGIES
CORPORATION, AND NAGRASTAR,
13 L.L.C.

14 UNITED STATES DISTRICT COURT
15 CENTRAL DISTRICT OF CALIFORNIA
16 SOUTHERN DIVISION
17

18
19 ECHOSTAR SATELLITE
CORPORATION, ECHOSTAR
20 COMMUNICATIONS
CORPORATION, ECHOSTAR
21 TECHNOLOGIES
CORPORATION, AND
22 NAGRASTAR L.L.C.

23 Plaintiffs,

24 v.

25 NDS GROUP PLC, NDS
26 AMERICAS, INC.,

27 Defendants.
28

No.

**AFFIDAVIT TESTIMONY
OF MARTIN PAUL STEWART**

1 **BEFORE ME**, the undersigned notary public, on this day personally
2 appeared **Martin Paul Stewart**, a person whose identity is known to me. After I
3 administered the oath to him, and being duly sworn, he stated as follows:

- 4 1. My name is Martin Paul Stewart. I was formerly known as, and am still
5 referred to at times as Martin "Marty" Mullen. I am over 18 years of age and
6 am duly competent in all respects to make this affidavit. The facts stated
7 herein are based upon my own personal knowledge, unless otherwise stated,
8 and are true, accurate to the best of my current knowledge, and correct. If
9 called to testify in the above styled and numbered cause, I would provide
10 sworn testimony in accordance with the facts stated herein.
- 11 2. I am the owner/operator of a business entity known as Multi-Media Images
12 ("MMI"). I started this business as a sole proprietorship in 1997. MMI was
13 formerly engaged in a wide variety of enterprises including: internet & new
14 media design; video productions; CD ROM presentations; audio production;
15 networking; network security analysis; and retail sales/installations of home
16 entertainment consumer electronics and Star Choice satellite systems. MMI
17 is currently engaged in security consulting providing these services to clients
18 including major Canadian banks, the medical industry and the Canadian
19 Department of Defense.
- 20 3. During the early years of operation MMI engaged in the sale and installation
21 of other satellite systems. Specifically, during that time MMI's satellite
22 business consisted of approximately 85% DirecTV systems, 10% DISH
23 Network systems and 5% C-Band systems. Of these satellite system sales,
24 approximately 20% were based upon what was commonly referred to as
25 'grey market' sales with the remaining approximately 80% consisting of
26 what was commonly referred to as 'black market' sales.
- 27 4. 'Grey market' sales consist of situations where satellite systems are sold to
28 consumers in an area, such as Canada, where a particular satellite system's

201

1 provider is not authorized to procure subscribers. 'Grey market' sales are set
2 up by the subscriber providing a valid credit card number and designating a
3 United States address for the purposes of billing such that the satellite system
4 provider is unaware of the subscriber's residence in an area not authorized to
5 pay the subscription fee for receiving that provider's signal.

6 5. 'Black market' sales consist of situations where the consumer purchases the
7 equipment necessary for the reception and decryption of a satellite system
8 provider's signal without paying the provider the requisite subscription fees.
9 'Black market' sales are set up by a consumer purchasing satellite
10 reception/decryption equipment (including what is known as an Access Card
11 or 'Smart Card') which has been altered, modified or 'pirated' such that the
12 consumer could receive, decrypt and view the provider's satellite signal
13 without paying the monthly fees.

14 6. Importantly, at the time MMI was established in or around February 1997,
15 the only method available for distributing satellite receivers for the DISH
16 Network signal was via the 'grey market' as, to my knowledge, no one had
17 been able to successfully procure the dump of the EchoStar/NagraStar ROM
18 Code yet.

19 7. After initially starting MMI in or around February 1997, MMI was
20 purchasing satellite receivers (or 'set-top boxes') from local area distributors
21 in Toronto, Canada. Two of the primary distributors were Tech Electronics
22 and Incredible Electronics.

23 8. With regard to the satellite systems set up under the 'black market' model,
24 Access Cards (or 'smart cards') which had been altered, modified or 'pirated'
25 were needed for these receivers to decrypt the particular provider's satellite
26 signal. Specifically, the Access Cards (or 'smart cards') needed to have
27 certain software loaded onto their microprocessors in order for them to allow
28 the receiver (or 'set-top box') to decrypt the encrypted satellite signal.

202

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

9. Initially, prior to May of 1996 while I was working/residing in the Cayman Islands, I was receiving some of these software-loaded pirated devices, as well as subsequent support for same to combat or overcome electronic counter measures ("ecm") directed at disabling these cards, from an individual named Gary Toscholke.

10. During this same period, I was placed in contact with an individual referenced as "the visitor" or "the European". I was placed in contact with this individual by a former business associate named Chuck 'Hauser'. This European, who spoke with a distinct German accent, was in the business of, among other things, providing software-loaded access cards that would facilitate the unauthorized decryption of a satellite provider's satellite signal. I was initially instructed by Chuck 'Hauser' to refer to this 'European' by the fictitious name of Martin. I later came to refer to this 'European' by another possibly fictitious name "Palma" or "Lorenzo Palma".

11. After initially being introduced to 'Palma', he advised that he was able to write software to satellite access cards which would allow the end-user/consumer to decrypt a satellite provider's encrypted satellite signal. 'Palma' requested that money be sent to the following address in order to receive these software loaded access cards: Lorenzo Palma, Pielle Electronica, Vicolo Vigneto o/c, 24030 Caprino Bergamasco BG, Italy.

12. In order for 'Palma' to communicate with me, he instructed me to set up several email accounts. Subsequently, he provided me with a DES encryption engine known as FSCRAM and instructed me to use this program to encrypt all communications with him. He further instructed me to begin each such encrypted communication with seemingly innocuous phrases such as: "Hi, how are you? Here is the recipe for the turkey dinner."

203

1 13. After 'Palma' provided me with the FSCRAM encryption software for
2 electronic communications, he advised that for \$45,000 he would guarantee
3 MMI future purchases of software-loaded DirecTV H-Cards that would
4 allow the end-user to obtain unauthorized access to the encrypted satellite
5 signal. 'Palma' was provided with this requested amount via Paul Cater,
6 Mike McAllister and Peter Beacock. Cater, McAllister and Beacock were
7 distributors of 'Palma's' software-loaded access cards.

8 14. After MMI was originally formed, 'Palma' continued to provide
9 software-loaded access cards for the DirecTV satellite system that were,
10 eventually, distributed to end-users who could then obtain access to the
11 encrypted satellite signal. Importantly, the software utilities provided by
12 'Palma' were somehow 'pre-loaded', 'prepped' or otherwise pre-equipped to
13 handle future ecm updates launched by NDS. Specifically, these utilities
14 were pre-equipped to handle ecm's when NDS updated the access cards to,
15 among others, 18-updates, 23-updates, 26-updates and 28-updates. As
16 explained more fully below, 'Palma' was able to pre-equip his utilities to
17 maintain the access cards he provided because he was an NDS
18 agent/employee and, as he candidly acknowledge to me, had full access to
19 both the inner workings of the card's microprocessor and prior knowledge of
20 upcoming ecm's. In addition, each time a new generation card was about to
21 be released, 'Palma' informed me that not to worry because he already had
22 the 'fix' for the new card prior to that new generation card to be released.

23 15. In or about December 1997 or January 1998 I became aware that
24 'Palma' was actually working for, and under the direct control of NDS.
25 Specifically, the day after 'Palma' had provided me with a supply of his
26 software-loaded access cards for distribution, he called me and inquired into
27 whether or not those access cards had already been released for distribution.
28 When I inquired into why he was asking, he told me that the following day

1 an ecm was going to be released that would disable these cards. After
2 informing 'Palma' that most of his cards had already been released to Paul
3 Cater. 'Palma' told us to get these cards back immediately and that he could
4 send a program that would correct the cards and defeat the upcoming ecm.
5 During this conversation, which was also heard by another individual present
6 with me at the time, I was able to clearly hear an intercom announcement in
7 'Palma's' background which stated words to the affect of would all "NDS
8 employees" please report immediately to the boardroom. 'Palma'
9 unsuccessfully attempted to cover the receiver on his phone to muffle the
10 announcement and then abruptly ended the conversation. Importantly, just as
11 'Palma' told me on the phone at that time, within the next few days an ecm
12 was released that effectively disabled 'Palma's' cards that we were unable to
13 recall.

14 16. In August 1997 I was contacted via telephone by an individual named
15 Oliver Kommerling. During this conversation, Kommerling introduced
16 himself to me and informed me that he would soon be in possession of the
17 first hack of the EchoStar/NagraStar ROM Code. Kommerling stated to me
18 that this ROM Code was currently being extracted in a highly sophisticated
19 labatory in Europe. Kommerling then informed me that he was able to offer
20 me the hack on the EchoStar/NagraStar microprocessor and that he wanted to
21 come to Canada and arrange a meeting to discuss the details. Kommerling
22 said that he was informed that I was in possession of pirating software for the
23 DirecTV H-Card and that if I delayed in releasing that software he was
24 authorized to provide me with the DISH Network ROM Code. It is my
25 understanding, after speaking with numerous individuals, including without
26 limitation, Kommerling's agent John Luyando (or "Yanni"), as well as
27 reading Kommerling's sworn declaration filed in support of the Canal+
28 litigation against NDS, that at the time Kommerling contacted me and stated

1 that he would provide me with the soon-to-be-completed EchoStar/NagraStar
2 ROM Code extraction, Kommerling was an NDS employee and was acting
3 on behalf of, and under the direct control of NDS.

4 17. After Kommerling's initial phone call to me, he sent me an email with
5 the following contact information: "O. Kommerling, 66484 Riedelberg, M
6 hlstr. 7, Germany, Tel: +49 6339 9219 11, or +49 6339 9219 44, Fax: +49
7 6339 9219 46, Cell: +49 1712 6446 80."

8 18. On Saturday August 23, 1997 at 11:03 a.m. I called Kommerling to
9 further discuss his offer. Using the information he provided me via email, I
10 contacted him through his cell number at + 49 1712 6446 80. (Attached to
11 this Affidavit as Exhibit A is a true and correct copy of a Bell Canada phone
12 record evidencing this call.)

13 19. My August 23, 1997 phone call to Kommerling lasted approximately
14 one (1) hour. During this conversation, Kommerling informed me that the
15 DISH Network hack was almost completed and that he would arrange a trip
16 to Canada in the immediate future to discuss details of his authority to sell
17 me the EchoStar/NagraStar ROM Code.

18 20. In October 1997 I was informed by Paul Cater that Kommerling and
19 an individual identified as Yanni (whose real name I know to be John
20 Luyando) traveled to Canada to meet with Cater, Mike McAllister and Peter
21 Beacock and discuss Kommerling's ability to provide the DirecTV hack and
22 for Kommerling to set up a meeting with me to discuss his offer to sell the
23 DISH Network hack. When I asked Yanni why they did not come and
24 discuss Kommerling's offer with me directly, he informed me that they were
25 'instructed' to go through Cater, McAllister and Beacock in order to get to
26 me. After speaking with Yanni on or about September 20, 2002, it is my
27 understanding that this 'instruction' came directly from NDS.
28

206

1 21. In February 1998 Kommerling contacted me again via telephone and
2 advised me that the DISH Network hack had been completed and that the
3 ROM Code had been fully extracted from the access card's microprocessor.
4 He further told me that Yanni would be contacting me within the next couple
5 of weeks to set up a meeting in Canada to discuss Kommerling's authority to
6 offer me this ROM Code. During this conversation Kommerling stated that
7 he was also able to provide me with support for the DirecTV H-card hack in
8 addition to providing us the DISH Network ROM Code, as long as I delayed
9 in releasing any software for the H-Card.

10 22. In accordance with Kommerling's statements to me, Yanni called me
11 in early March of 1998 and arranged a meeting to discuss Kommerling's
12 offer of the DISH Network ROM Code. This meeting took place on Friday
13 March 13, 1998 at the Hilton hotel in Windsor, Ontario. Myself, Archie
14 Timuik and Joseph Lucker were in attendance at this meeting with Yanni
15 (John Luyando). Yanni informed us that Kommerling could not be in
16 attendance at the meeting because of work conflicts, but that Kommerling
17 had bestowed full authority on Yanni to negotiate Kommerling's offer of the
18 DISH Network hack.

19 23. During this meeting Yanni informed us that Kommerling was
20 authorized to offer us the DISH Network ROM Code for \$1,000,000. During
21 this March 13, 1998 meeting, Yanni informed us that Kommerling was
22 willing to either set up a demonstration of the DISH Network hack, or
23 provide us with a portion of the EchoStar/NagraStar ROM Code so that we
24 could verify that Kommerling was in fact in possession of the hack.

25 24. After lengthy negotiations took place at this March 13, 1998 meeting,
26 we were ultimately unable to come to any mutually agreeable terms
27 regarding Kommerling's offer to sell us the DISH Network hack. However,
28 Yanni informed us that he would pass our counter-offer on to Kommerling

207

1 and get back with us. It is my understanding, after speaking with numerous
2 individuals, including without limitation, Kommerling's agent John Luyando
3 (or "Yanni"), as well as reading Kommerling's sworn declaration filed in
4 support of the Canal+ litigation against NDS, that at this time Kommerling
5 was an NDS employee and was acting on behalf of, and under the direct
6 control of NDS.

7 25. During the period from the March 13 ,1998 meeting until the end of
8 April 1998 I received several phone calls from Yanni. Yanni advised me that
9 Kommerling was unable to sell us the DISH Network hack for anything less
10 than his stated price of \$1,000,000. It is my understanding, after speaking
11 with numerous individuals, including without limitation, Kommerling's
12 agent John Luyando (or "Yanni"), as well as reading Kommerling's sworn
13 declaration filed in support of the Canal+ litigation against NDS, that at this
14 time Kommerling was an NDS employee and was acting on behalf of, and
15 under the direct control of NDS.

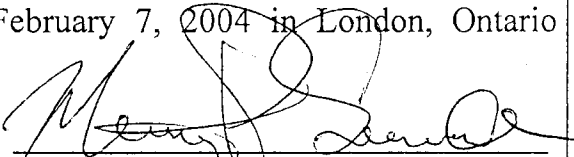
16 26. Because we were unwilling to provide Kommerling with the entire
17 \$1,000,000 upfront, negotiations came to an end. Shortly thereafter, I
18 learned through common knowledge in the satellite pirating community, as
19 well as through Al Menard's www.dr7.com website and Chris Tarnovsky's
20 postings on same, that this DISH Network ROM dump had been provided to
21 another group known as the 'Swiss Cheese' Group.

22 27. I swear under the penalties of perjury pursuant to the laws of the
23 United States of America that the foregoing is true and correct and is based
24 upon my own personal knowledge.
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

Further Affiant sayeth not.

Sworn, subscribed to and executed on February 7, 2004 in London, Ontario
Canada.


Martin Paul Stewart

SWORN TO and **SUBSCRIBED** before me by
Martin Paul Stewart on February 7, 2004.


Notary Public in and for the
City, Town of London, Province of Ontario,
Country of Canada

My commission expires: n.a.

209

1 SQUIRE, SANDERS & DEMPSEY L.L.P.
Michael T. Purleski (State Bar No. 216307)
2 Angela N. O'Rourke (State Bar No. _____)
801 S. Figueroa St., Fourteenth Floor
3 Los Angeles, California 90017
Telephone: (213) 624-2500
4 Facsimile: (213) 623-4581

5 T. WADE WELCH & ASSOCIATES
T. Wade Welch (*pro hac vice*)
6 Ross W. Wooten (*pro hac vice*)
Joseph H. Boyle (*pro hac vice*)
7 2401 Fountainview Suite 700
Houston, Texas 77057
8 Telephone: (713) 952-4334
Facsimile: (713) 952-4994

9 Attorneys for Plaintiffs
10 ECHOSTAR SATELLITE
CORPORATION,
11 ECHOSTAR COMMUNICATIONS
CORPORATION, ECHOSTAR
12 TECHNOLOGIES
CORPORATION, AND NAGRASTAR,
13 L.L.C.

14 UNITED STATES DISTRICT COURT

15 CENTRAL DISTRICT OF CALIFORNIA

16 SOUTHERN DIVISION

17
18 ECHOSTAR SATELLITE
CORPORATION, ECHOSTAR
19 COMMUNICATIONS
CORPORATION, ECHOSTAR
20 TECHNOLOGIES
CORPORATION, AND
21 NAGRASTAR L.L.C.

22 Plaintiffs,

23 v.

24 NDS GROUP PLC, NDS
AMERICAS, INC.,

25 Defendants.
26
27
28

No. SA CV 03-950 DOC(ANx)

DECLARATION OF
REGINALD SCULLION

Date:

Time:

Dept: Judge David O. Carter
Courtroom 9-D

1 BEFORE ME, the undersigned notary public, on this day, personally
2 appeared Reginald "Reg" Scullion, a person whose identity is known to me. After I
3 administered the oath to him, and being duly sworn, he stated as follows:

4 1. My name is Reginald Scullion. I am over 18 years of age and am duly
5 competent in all respects to make this affidavit. The facts stated herein are
6 based upon my own personal knowledge, unless otherwise stated, and are
7 true, accurate, to the best of my current knowledge, and correct. If called to
8 testify in the above styled and numbered cause, I would provide sworn
9 testimony in accordance with the facts stated herein.

10 2. I have been involved in the satellite television business generally since
11 approximately 1980 owning a satellite installation and receiver repair
12 business. I temporarily retired from the satellite business in 1994 due my
13 pursuit of other business opportunities, in addition to personal health issues,
14 among other reasons. I returned to the satellite business in approximately
15 July 1996 whereupon I went back into the satellite sales and service industry.

16 3. Upon my return to the satellite sales and service industry in approximately
17 the middle of 1996, I began selling DBS systems for the DirecTV satellite
18 system. I purchased my products from distributors such as DSI, New
19 Advanced Technologies, and Zed Marketing, among others. I sold DirecTV
20 products locally and over the Internet. I also installed the DBS systems for
21 my customers and assisted in the activation of the customers' DirecTV
22 subscription accounts. For activation assistance, I dealt with grey marketers,
23 specifically New Advanced Technologies in Quebec and Zed Marketing in
24 Ontario. I was involved in selling systems with both altered and unaltered
25 Access Cards which were both believed to be legal in Canada due both to the
26 reading of the law and to Canadian court rulings which constantly said that it
27 was legal to decode systems that were not those of authorized distributors in
28

1 Canada. I would obtain the hacked cards from my DirecTV distributors
2 and from grey marketers in Canada. Hacked DirecTV Access Cards were
3 sold very openly at that time since they were considered to be totally legal.
4 Since I was quite knowledgeable with computers, I was also writing some of
5 my own code for the DirecTV Access Cards and was programming my own
6 DirecTV Access Cards which were purchased directly from DirecTV on my
7 behalf and for this purpose. I also had manufactured my own "green cards"
8 and programmers/unloopers, bootstrap writers, and other signal reception
9 devices, deemed legal in Canada. I had purchased a large quantity of
10 DirecTV Access Cards through various authorized DirecTV dealers who
11 were actually Canadians known to DTV such as Z-Marketing and others and
12 those cards came directly from DirecTV.

13 4. On or about November 4, 1998, my business (Avantec, Inc.) was raided by
14 the Royal Canadian Mounted Police ("RCMP"). As a result of the raid, the
15 RCMP seized (1) satellite and non-satellite equipment, (2) approximately
16 \$5.5 million dollars in my bank accounts and safety deposit boxes belonging
17 to me and several other members of my family, and (3) approximately 12,000
18 new DirecTV Access Cards purchased from DTV. The Canadian
19 government is still in possession of these seized items.

20 5. I am currently the owner and operator of a website named www.legal-
21 rights.org, which focuses primarily on the anti-piracy of satellite television
22 systems in Canada and the United States in addition to general news,
23 publications, commentaries, and updates on the battle against satellite piracy.

24 6. I am also currently an Administrator on several other websites including
25 www.piratesden.com, www.outermatrix.com, www.dsschat.com,
26 www.freedomfight.ca, and www.digital-law.org, among others. My
27 responsibilities as an Administrator include reviewing, controlling, deleting,
28

1 and banning certain persons and/or posts on the websites which may contain
2 offensive, illegal, and/or inappropriate material.

3 7. Due to my status as an Administrator on these websites, among others, I have
4 and/or had complete access to the control panels on all of these websites,
5 among others, which enables me to view all of the information that members
6 and other Administrators post in their registration sheets, as well as, all
7 related information obtained on these people which is stored in the websites'
8 databases. A member's personal information provided in their registration
9 sheet is also often useful in obtaining additional information related to that
10 person from other websites since people are often members of several
11 different website forums at the same time and members often use the same
12 password from website to website. Accordingly, members' IP addresses, real
13 names, and much other information can be obtained by cross-referencing the
14 members' information in different forums. In this way I can be sure that a
15 person on one web site is the same person as uses a different Nick on a
16 different website.

17 8. Through my work as an Administrator on pirate websites and forums, I
18 initially became familiar with Christopher Tarnovsky ("Tarnovsky") in
19 approximately middle of 1996 and engaged in numerous telephone and email
20 correspondence exchanges regarding satellite piracy.

21 9. In or about late 1996, Tarnovsky was working with Ron Ereiser ("Ereiser")
22 in Kerrobert Manitoba developing and distributing "battery cards." Shortly
23 after the "battery card" release, Tarnovsky and Ereiser abandoned their
24 customers and refused to provide support for the "battery cards" for a few
25 months. At some time thereafter, "L-cards" and "T-cards" were released to
26 compensate for this lack of support in the battery cards. I decided to provide
27 support for the "L-cards" and "T-cards" in terms of coding and programming,
28

1 in part, because Tarnovsky and Ereiser had abandoned people and were not
2 providing technical support for these cards. In fact, Tarnovsky accused me of
3 stealing his code from the "battery card" because Tarnovsky knew that the
4 DS5000 DALLAS chip on the "L-Card" could be pulled, and thus a good
5 programmer could reprogram the file to support "battery cards" he had
6 designed by Norman Dick; however, this was not the case and I did not steal
7 Tarnovsky's code. As a result of Tarnovsky and Ereiser abandoning people
8 and not providing technical support for the "L-cards" and "T-cards," and my
9 subsequent decision to support these persons and devices, Tarnovsky and I
10 became arch enemies starting in approximately October 1996. Accordingly,
11 Tarnovsky spent a lot of time on the Internet chat rooms and forums
12 criticizing me and calling me names thinking I was dumping his cards.

13 10. As a result of my providing support and my disagreements with Tarnovsky,
14 on or about January 29, 1997, Tarnovsky, using the nickname "biggun," sent
15 me an email from "bg@wbm.ca" wherein he threatened me and established
16 his relationship with NDS, formerly NDC. (Attached hereto as Exhibit A.)
17 Tarnovsky's email stated, among other things, "[i]f I am against you, you
18 will not have happy customers under your side. I give you the tv and I can
19 remove the tv." Concerning my failure to respond to his offer, Tarnovsky
20 stated that if he did not hear back from me, he would "consider you
21 [Scullion] a threat to me [Tarnovsky] and commence something very drastic
22 soon after. I may just give the source to NDC. I am sure they will purchase
23 it from me and if I agree to stop, then your world stops also . . . You could
24 have been a distro. point for us . . Instead you are a thefe." Tarnovsky then
25 signs off, "bye! biggun." At this time, I came to believe that Tarnovsky had a
26 relationship with NDC and/or NDS.

27 11. In or about fall 1998, Al Menard ("Menard"), owner and operator of
28

1 www.dr7.com, first approached me wherein he informed me that he was
2 involved in a plan to be the Canadian leader in distributing Pirated EchoStar
3 Access Cards. Menard inquired as to whether I was interested in participating
4 in his distribution network. I declined his offer.

5
6 12. Shortly thereafter, Tarnovsky disappeared entirely from the IRC forums. In
7 approximately September 1998, I noticed that Tarnovsky had reemerged and
8 began posting and chatting on www.dr7.com website under the nickname
9 "Swiss Cheese Productions" ("SCP"). The "SCP" consisted of Tarnovsky
10 and Menard who had sub-distributors acting at the direction and supervision
11 of Menard. The "SCP" initially posted certain EchoStar "freeware" (which is
12 software that people do not need to pay for as it is offered "free" on the
13 Internet on the website www.dr7.com. I did not pay much attention to
14 "SCP's" operations and the freeware posts because they were directed at the
15 EchoStar system, a system that I was not interested in and/or involved with,
16 and a system that no known hack was available for at that time, even though
17 Tarnovsky and Menard were promising a release of the hack shortly.

18 13. On or about early 1999, Menard personally contacted me by telephone
19 wherein he invited me to become a moderator on his website, www.dr7.com.
20 Shortly thereafter, I was made an Administrator. Consistent with my current
21 responsibilities as an administrator on the current websites that I am an
22 Administrator on, my responsibilities as both a Moderator and an Administer
23 on Menard's website, www.dr7.com, included reviewing, controlling,
24 deleting, and banning certain persons and/or posts on the website. At or
25 about the same time, I was also an Administrator on both a DSS chat
26 (www.risestar.com) and Sean Quinn's website (www.hitecsat.com). As a
27 result of my Administrator position, I had possession of certain users'
28

1 passwords and could access their accounts. For example, I had passwords
2 that belonged to Tarnovsky, Sean Quinn, and Dave Dawson.

3 14. Shortly thereafter, on or about early 1999, I verified that Tarnovsky was part
4 of the "SCP." I initially discussed particular chat posts made by "SCP" with
5 other administrators on a private forum chat on the DR7 website wherein I
6 commented about the similarities between "SCP" and Tarnovsky's previous
7 posts he made as using other nicknames including, but not limited to,
8 "Scatman Cran," "Von," "Vonrola," "Big Gun," "Shrimp," and "Nipper."
9 Shortly thereafter, I also reviewed the information on "SCP's" profile and
10 compared the passwords and IP addresses of "SCP" with that of Tarnovsky's
11 other nicknames including, but not limited to, "Scatman Cran," "Von,"
12 "Vonrola," "Big Gun," "Shrimp," and "Nipper." The results of such a search
13 revealed that "SCP's" and Tarnovsky's other nicknames' and IP addresses
14 were identical and that the same anonymizer was used for both when they
15 differed.

16 15. Tarnovsky also registered the nicknames Von, Vonrola, and Nipper on the
17 DR7 website on the same day. I have personal knowledge of this fact
18 because, due to my status as administrator which allowed me to access
19 particular files and databases on the DR7 website, I had full access to the
20 Control Panel which showed all registrations, IP addresses, and complete
21 information on all of the members of the DR7 website. Although these files
22 do not contain specific "CHRISTIAN " names, one can confirm the identity
23 of certain users by cross-referencing email addresses and passwords
24 contained in users' registration profiles. Moreover when people post, the IP
25 address they use can be determined and traced back to the actual person.
26 Examples of registration profiles of Tarnovsky's aliases include, but are not
27 limited to, the following information: (a) Von | phoenix
28

1 | |von@fumanche.net|http://| Write|| |3| Junior Member|||no|; (b) VONrola
2 | |hello| |vonrola@fumanche.net| | [|http://www.vegetablesRus.com|](http://www.vegetablesRus.com|) W rite
3 | |Lowlife dweeb on drugs| |1|Junior Member |Fucking with Vegetable
4 | Scallion||yes|; and (c) nipper |nipper ||charlie@dicknetwork.sux|
5 | [|http://|](http://|)Write|||16|Junior Member|||yes|. As a result of my investigation, it was
6 | revealed that Tarnovsky was using the nickname Nipper.
7 |

8 | 16. My investigation as to the identity of Tarnovsky being the same person who
9 | was using the nicknames “SCP,” “Scatman Cran,” “Von,” “Vonrola,” “Big
10 | Gun,” “Shrimp,” and “Nipper,” among others, was further strengthened once
11 | Menard instructed me to no longer perform my administration duties,
12 | including monitoring, with respect to any posts made by Tarnovsky, “SCP,”
13 | “Scatman Cran,” “Von,” “Big Gun,” “Shrimp,” or “Nipper,” among other
14 | known nicknames used by Tarnovsky.

15 | 17. On or about April 1999, Menard approached me a second time to solicit my
16 | participation in his distribution network to sell Pirated EchoStar Access
17 | Cards. During this conversation, Menard informed me that he was “close to
18 | receiving a full hack of the EchoStar system” and, because of the pirate
19 | community’s past interest in Swiss Cheese Production’s products, Menard’s
20 | distribution plan was a guaranteed money maker. Menard also informed me
21 | that the distribution network was going to have something special attached
22 | with its operation: the protection and control of NDS. Menard informed me
23 | that NDS was the entity whom had ordered the hack and the distribution of
24 | Pirated EchoStar Access Cards through Menard’s distribution network via
25 | Tarnovsky. Menard informed me that NDS had an arrangement with
26 | Tarnovsky to provide the support and facilitation of the hacked EchoStar
27 | ROM Code to be sent to Menard to be used in the distribution network.
28 |

1 Menard also informed me that I had nothing to worry about with respect to
2 being raided by the RCMP due to the fact that NDS would be running
3 interference in the distribution network and that NDS was connected and had
4 a solid relationship with the RCMP. Menard then instructed me to get over
5 my prior disagreements with Tarnovsky because this was such a good deal
6 that I should not pass up.

7
8 18. On or about November 1999, I spoke with Menard wherein he informed me
9 that the Pirated EchoStar Access Cards were "ready to be distributed to the
10 public," he had certain vendors in place, and that he wanted me to be one of
11 those vendors. Menard informed me that the vendors who had agreed to
12 participate in the distribution network included Sean Quinn (a/k/a "Hitec"
13 d/b/a www.hitecsat.com), Andre Sergei (a/k/a "Koin" d/b/a
14 www.koinvizion.com), Dave Dawson (a/k/a "JD," "Jack Daniels," "John
15 Gotti," and "Teflon Don" d/b/a www.discountsatellite.com and
16 www.dsscanada.com), and Stan Frost (a/k/a "Frosty" and "Wheels" d/b/a
17 www.thenewfrontiergroup.com).

18 19. During this November 1999 discussion, Menard informed me that his role in
19 the distribution network was that of the reprogrammer and that he had four
20 vendors (Quinn, Sergei, Dawson, and Frost, among others) who agreed to be
21 the persons responsible for delivering EchoStar Access Cards to Menard.
22 Once received, Menard would use the equipment he was provided with and
23 received from NDS via Tarnovsky to reprogram, update, and otherwise load
24 EchoStar's Code onto the Access Cards (which resulted in the Access Card
25 becoming "hacked" or "pirated" thus enabling the user to receive
26 unauthorized DISH Network television programming). I specifically recall
27 other Administrators on Menard's DR7 website requesting from Menard that
28

1 he reprogram EchoStar Access Cards for them. Menard would respond by
2 requesting that the Administrators send the cards to him and, once the Access
3 Cards had been reprogrammed, Menard would return the Pirated EchoStar
4 Access Cards to the vendor who, in turn, would return the card to the
5 customer to complete the transaction. These transactions occurred between
6 Canada and the United States, among other places. Customers were charged
7 approximately \$300-400 USD which payment was sent from the United
8 States to Canada, among other places.

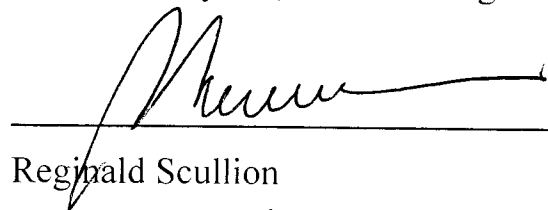
9 20. In fact, Quinn ("Hitec") told me on numerous occasions that he was traveling
10 to Menard's place of business in order to deliver EchoStar Access Cards for
11 reprogramming in furtherance of their distribution network.

12 21. Although I did not want to tell Menard ("DR7") much about my personal
13 affairs, I was not interested in working in his distribution network because I
14 had sold my business and was no longer interested in selling any products in
15 the satellite piracy business. As a result, I respectfully declined his offer.

16 22. I have received approximately 20 emails from Tarnovsky and approximately
17 50-100 emails from Menard that support the facts as stated herein.

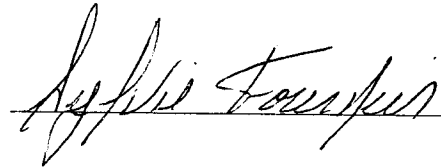
18
19 Further Affiant sayeth not.

20 Sworn, subscribed to, and executed on February 16, 2004 in Rigaud, Quebec
21 Canada.

22
23 
Reginald Scullion

24
25 **SWORN TO and SUBSCRIBED** before me by
26 on February 17, 2004.



27
28 

IRE, SANDERS L.L.P.
1 South Figueroa Street
14th Floor

DECLARATION OF REGINALD SCULLION

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

Notary Public in and for the
Town of Rigaud, Province of Quebec,
Country of Canada

My commission expires: December 8, 2006

Message-ID: <32EF6D4E.403B@wbm.ca>
Date: Wed, 29 Jan 1997 10:31:26 -0500
From: bg <bg@wbm.ca>
X-Mailer: Mozilla 3.01Gold (WinNT; I)
MIME-Version: 1.0
To: Reg Scullion <regs@total.net>
Subject: No response. Time finished..
References: <v03007800af0dd2ed8fcd@[205.236.86.22]>
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=us-ascii
X-UIDL: 2481db0946cb23d4aea057df26818398
Reg,

You have chosen to ignore me an no reply since your last message. I begin to think you accept my proposititon to you and make things nice for both of us. If I am against you, you will not have happy customers under your side. I give you the tv and I can remove the tv. I have been very patient with you and my patient is now expireing. You have until 1800hrs my time! (This is 1200 for you.) If I do not hear from you before I go to my school, I will consider you a threat to me and commence something very drastic soon after. I may just give the source to NDC. I am sure they will purchase it from me and if I agree to stop, then your world stops also. You leave me no other choice. I also know one of people with the .hex file has given this to you. Perhaps for some money. I am not sure. This is not fair to me. You could have been a distro. point for us.. Instead you are thefe.

je attendre sur toi alors!
bye!

biggun

p.s.- I have my Sky TV to enjoy! So, DSS is a simple part time work!
--

EXHIBIT

4

Exhibit
"A"

22/

PROOF OF SERVICE

I, Villirie Harmon, declare:

I am a resident of the State of California and over the age of eighteen years, and not a party to the within action; my business address is 801 South Figueroa Street, 14th Floor, Los Angeles, CA 90017-5554. On February 18, 2004, I served the within documents:

EchoStar Satellite Corporation's Second Amended Complaint

X by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at Los Angeles, California addressed as set forth below.

by causing personal delivery of the document(s) listed above to the person(s) at the address(es) set forth below.

by placing the document(s) listed above in a sealed envelope and affixing a pre-paid air bill, and causing the envelope to be delivered to Federal Express for delivery overnight.

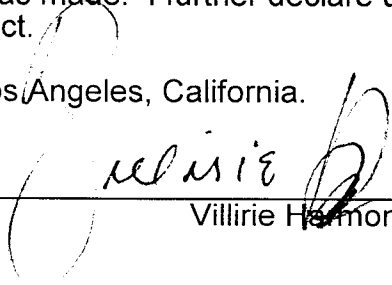
By transmitting via facsimile the document(s) listed above to the fax number(s) set forth below on this date.

Darin W. Snyder
David R. Eberhart
O'Melveny & Myers LLP
Embarcadero Center West
275 Battery Street
San Francisco CA 94111-3305

Patrick Lynch
Maitreya Jani
O'Melveny & Myers LLP
610 Newport Center Drive, 17th Floor
Newport Beach CA 92660-6429

I am readily familiar with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit. I declare that I am employed in the office of a member of the bar of this court at whose direction the service was made. I further declare under the penalty of perjury that the foregoing is true and correct.

Executed on February 18, 2004, at Los Angeles, California.



Villirie Harmon