T. WADE WELCH & ASSOCIATES
Chad M. Hagan (*pro hac vice*)
chagan@twwlaw.com
2401 Fountainview, Suite 700
Houston, Texas 77057
Telephone: (713) 952-4334
Facsimile: (713) 952-4994

DLA PIPER US LLP
David A. Grenardo (State Bar No. 223142)
david.grenardo@dlapiper.com
1999 Avenue of the Stars, 4th Floor
Los Angeles, California 90067
Telephone: (310) 595-3031

Attorneys for Plaintiffs
ECHOSTAR SATELLITE CORP., et al.

**UNITED STATES DISTRICT COURT**
**CENTRAL DISTRICT OF CALIFORNIA**
**SOUTHERN DIVISION**

ECHOSTAR SATELLITE CORP., et al.,

Plaintiffs/ Counterclaim Defendants,

v.

NDS GROUP PLC, et al.,

Defendants/ Counterclaim Plaintiffs.

No. SA CV 03-950 DOC(JTLx)

**ECHOSTAR'S FIFTH AMENDED COMPLAINT (5AC) 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 Communications Act of 1934, as amended, 47 U.S.C. § 605(a);**

4) **Violation of RICO Statute, 18 U.S.C. § 1962(c);**

5) **Unfair Competition in Violation of California Business & Professions Code § 17200;**

6) **Violation of California Penal Code § 593d(a);**

7) **Violation of California Penal Code § 593e(b);**

**JURY TRIAL DEMANDED**

# TABLE OF CONTENTS


I. INTRODUCTION & NATURE OF THE CASE ..... 1

II. JURISDICTION & VENUE ..... 10

III. PARTIES & RELATIONSHIP TO PLAINTIFFS' SUIT ..... 11

IV. RELATIONSHIP BETWEEN DEFENDANTS AND THEIR EMPLOYEES, AGENTS, SUB-AGENTS AND CO-CONSPIRATORS ..... 13

A. Direct Employment Relationship ..... 14

B. Agency Relationships ..... 14

1. Agency/Sub-Agency ..... 14

a. Menard ..... 14

b. Dawson, Quinn, Sergei, and Frost ..... 15

c. Mervin Main ..... 16

C. Agency by Ratification ..... 16

D. Co-Conspirators of NDS Group and NDS Americas ..... 17

V. PLAINTIFFS' & DEFENDANT NDS'S SECURITY SYSTEMS ..... 18

A. The Components of Plaintiffs' Security System ..... 18

B. NDS was Fully Compromised as Early as 1995 and Was Losing Credibility in the Conditional Access System Market Place ..... 20

C. At DirecTV's Request, in 1998 the Kudelski Group Competed With NDS for a Bid to Replace NDS's Security System With Nagravision as the Security System to be Used by DirecTV .... 21

VI. DEFENDANTS' CONCERTED OR OTHERWISE INTERRELATED UNLAWFUL CONDUCT ..... 22

A. PHASE 1: NDS Hires the World's most Infamous Hackers in order to "Control" the Hacking of its Access Cards and Security System -- in Lieu of Improving its Technology ..... 22

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

B. PHASE 2: NDS Turns These Same Pirates on its Competitors, Including Plaintiffs, in an Unlawful Attempt to Control the Piracy of its Competitors and, Ultimately, to Destroy the Competition... .... 27

1. Step 1: With the Assistance of Kommerling, NDS Built a Sophisticated Laboratory in Haifa, Israel, Where NDS Hacked Plaintiffs' Access Card and Extracted Plaintiffs' Secret and Proprietary ROM and EEPROM Codes..... 27

2. Step 2: NDS Provided their Hack Methodology to a Pirate Engineer Capable of Reprogramming Access Cards..... 28

a. NDS Used its Employee and Infamous Hacker, Tarnovsky, to Reprogram Plaintiffs' Access Cards Once NDS Developed Their Hack Method ..... 28

b. NDS Approached Others to Facilitate in the Proliferation of Plaintiffs' Security System..... 29

c. NDS and Tarnovsky Designed and Built the "Stinger" that NDS, Tarnovsky, and Menard Used to Control and Monopolize the Sales and Distribution of the unlawfully reprogrammed Access Cards over the Internet. ..... 30

3. Step 3: NDS, Tarnovsky, Menard and others Conspired to Place Pirated EchoStar Access Cards into the Black Market in a "Controlled" Manner and to Provide Technical Support for Same..... 31

a. NDS, through its Employees/Agents Tarnovsky and Menard, Created a Distribution Network Illegally Altered Access Cards and Other Circumvention Devices Designed to Thwart Plaintiffs' Security System. ..... 31

4. Step 4: NDS Sought to Eliminate Plaintiffs from the CAS Marketplace ..... 34

VII. PLAINTIFFS HAVE BEEN, AND CONTINUE TO BE, SUBSTANTIALLY INJURED BY DEFENDANTS' ILLEGAL CONDUCT ..... 40

VIII. PLAINTIFFS' MOTION TO INTERVENE IN THE *CANAL+ V. NDS* LITIGATION..... 41

IX. OUTLINE OF WRONGFUL CONDUCT AND THEORIES OF LIABILITY UNDERLYING PLAINTIFFS' CLAIMS..... 43

A. NDS Group..... 43

B. NDS Americas ..... 44

C. Menard and the NDS Distributors Dawson, Quinn, Sergei and Frost .... 47

D. Mervin Main ..... 48

X. CAUSES OF ACTION ..... 48

First Cause of Action:
(Circumventing Technological Measures Concerning Protected and Copyrighted Works in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1)(A)) ..... 48

Second Cause of Action:
(Manufacture of and Traffic in Signal Theft Technology and Devices in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2) ..... 50

Third Cause of Action:
(Facilitating the Unauthorized Reception of Satellite Signals in Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a)) ..... 52

Fourth Cause of Action:
(RICO, 18 U.S.C. § 1962(c)) ..... 54

Fifth Cause of Action:
(Unfair Competition, California Business & Professions Code § 17200) ..... 71

Sixth Cause of Action:
(Violation of California Penal Code § 593d(a)) ..... 73

Seventh Cause of Action:
(Violation of California Penal Code § 593e(b)) ..... 74

PRAYER FOR RELIEF ..... 76

DEMAND FOR JURY TRIAL ..... 81

EchoStar Satellite L.L.C., EchoStar Communications Corporation, EchoStar Technologies Corporation and NagraStar LLC ("EchoStar" or "Plaintiffs") hereby file their Fifth Amended Complaint ("5AC") against Defendants NDS Group PLC and NDS Americas, Inc. ("NDS" or "Defendants") and, in support thereof, respectfully state the following:

## I. INTRODUCTION & NATURE OF THE CASE

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

2. In order to protect its signal from unlawful and unauthorized use, a DBS provider must encrypt its satellite signal. EchoStar encrypts its satellite signals using a technology provided by NagraStar. NagraStar is a supplier of "smart cards" or access cards ("Access Cards") which contain tiny microprocessors embedded therein that facilitate functions of a larger "conditional access system" ("CAS") known as Digital Nagra Advanced Security Process ("DNASP"). DNASP uses a complex encryption system that is combined with a Digital Video Broadcasting ("DVB") scrambler/encoder system to form EchoStar's management and security system ("Security System"). EchoStar's Security System serves two interrelated functions: (1) subscriber management – allowing EchoStar to "turn on" Programming that a customer has ordered; and (2) encryption – preventing individuals or entities who have not ordered Programming from receiving it.

3. Defendants NDS Group PLC and NDS Americas, Inc. ("NDS") are the only major competitor of Plaintiff NagraStar in the CAS marketplace. NDS provides the encryption technology used by DirecTV. DirecTV is Plaintiff EchoStar's only major competitor in the U.S. DBS industry.

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

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

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

7. In sum, NDS was on the verge of losing one of its largest accounts, DirecTV, and ultimately, its ability to effectively compete in the CAS industry. Indeed, NDS internal documents cited herein are illustrative of NDS's knowledge of the vulnerability of its conditional access system, the real and immediate threat of losing its clients (*e.g.*, DirecTV) to its competitors, such as NagraStar, and that

high level executives in charge of NDS's security division had their "jobs in jeopardy." NDS knew it needed to act, and act quickly, if it was to have any chance of commercial survival.

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

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

10. Once NDS was able to put enough legal pressure on the pirating community, it began to recruit the hackers responsible for compromising NDS's technology and put them on the NDS payroll. Specifically, from as early as 1998, NDS employed, protected, paid, and controlled well-known satellite pirates and hackers including, but not limited to, Christopher Tarnovsky and Oliver Kommerling. With these notorious hackers on their payroll, and acting under the protective umbrella NDS provided them, NDS was now able to "control" the piracy of its clients. NDS capitalized on this fact by charging its clients various fees for combating the piracy of their CAS which NDS was controlling. Accordingly,

Phase 1 of the NDS plan to conquer the CAS marketplace was complete.

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

12. Step 1 required NDS to obtain the Read Only Memory ("ROM") and Electronically Erasable Programmable Read Only Memory ("EEPROM") codes ("Codes") used in their competitors' Access Cards. These proprietary codes form the heart and soul of CAS providers' security system and, as such, are secured and embedded in the tiny microprocessor unit stored in the Access Card. To extract these Codes, NDS needed a state-of-the-art laboratory, extremely sophisticated equipment including a scanning electron microscope and focused ion beam, and highly skilled engineers. There are only approximately six (6) of these labs in the world – NDS owns one of them in Haifa, Israel, which was designed and built by NDS with the assistance of Kommerling[1] and used by NDS to extract the ROM and EEPROM Codes and keys utilized by NDS's competitors.

13. Using its Haifa laboratory, NDS unlawfully and impermissibly cracked Plaintiffs' Access Card and extracted Plaintiffs' secret proprietary ROM and EEPROM Codes secured therein. NDS then used that information to develop a hack methodology to attack and defeat EchoStar's CAS. This was not the first time NDS engaged in this unlawful conduct. On April 9, 2002, NDS employee/agent Kommerling provided sworn testimony in another suit[2] brought by Canal+ against NDS for anticompetitive conduct similar to the acts alleged herein. In his

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

[2] Plaintiffs first attempted to assert their claims against NDS by moving to intervene in the *Canal+ v. NDS* litigation. NDS settled with Canal+ prior to Plaintiffs' Motion to Intervene being granted by the Court at which time Plaintiffs immediately filed this action.

declaration, Kommerling explained the methods NDS used to break the security system of Canal+ and to subsequently distribute that information to foster the satellite piracy of the Canal+ system.

14. Step 2 involved NDS transferring these unlawfully extracted ROM and EEPROM Codes to a pirating software engineer capable of using them to unlawfully access, reprogram, modify, alter, or otherwise interfere with the Access Cards used by Plaintiffs to protect the DISH Network satellite signal. NDS accomplished this task by using one of its new hacker employees, Tarnovsky, who had previously been responsible for compromising the CAS provided by NDS to DirecTV. NDS had recently moved Tarnovsky to California. Accordingly, NDS transmitted Plaintiffs' ROM and EEPROM Codes to Tarnovsky via Reuven Hasak (Israel) and John Norris (California), both of which were/are NDS employees. Tarnovsky has previously admitted to Kommerling that NDS provided Tarnovsky with Plaintiffs' ROM and EEPROM Codes via Hasak and Norris. In a similar vein, on or about October 5, 2001, Tarnovsky also admitted to Gilles Kaehlin, Head of Security for Canal+, that NDS was behind the Canal+ hack and that NDS provided Tarnovsky with the full Canal+ ROM code via Hasak and Norris.

15. At the direction and under the control of NDS, and with assistance provided by NDS, Tarnovsky was able to use Plaintiffs' proprietary Codes to design and build a pirating device that was capable of reprogramming Plaintiffs' Access Cards thereby allowing others to gain unauthorized and unlawful access to Plaintiffs' satellite television Programming services. NDS and Tarnovsky named this reprogrammer "the stinger."

16. Step 3 involved NDS distributing these illegally reprogrammed and pirated EchoStar Access Cards to the pirating community in a "controlled" manner. To accomplish this, NDS, via Tarnovsky, enlisted the assistance of Allen Menard and his hacker website, www.dr7.com. With the assistance of NDS and Tarnovsky, Menard set up a "controlled" distribution network consisting of a limited number of

dealers through which NDS and Tarnovsky could traffic and distribute the reprogrammed and pirated EchoStar Access Cards. Through these distribution dealers – Dave Dawson, Sean Quinn, Andre Sergei, and Stanley Frost, among others – NDS, Tarnovsky, and Menard could "control" the number of pirated EchoStar Access Cards that were being distributed to the pirating public.

17. Menard and Tarnovsky approached other individuals to help facilitate and promote the overriding NDS conspiracy. By way of example, in April 1999, and then again in November 1999, Menard approached Reginald Scullion with an offer to participate in the "DISH Network" hack and distribution scheme. During these conversations, Menard informed Scullion that, among other things: (a) NDS was behind the EchoStar hack; (b) the Tarnovsky/Menard distribution model would be protected and controlled by NDS; (c) NDS had an arrangement with Tarnovsky to provide the technical and software support and facilitate the hacked EchoStar ROM Code to be sent to Menard and used in the distribution network; and (d) NDS would protect this distribution network from potential RCMP raids.

18. NDS and Tarnovsky were able to control the distribution of these pirated EchoStar Access Cards because the "stinger" developed by NDS and Tarnovsky, and subsequently provided to Menard, would only reprogram a predetermined number of Access Cards before it would lock up.[3] At that point, Menard would send cash payments to Tarnovsky in California, via a forwarding mailbox Tarnovsky set up in Texas, which was concealed inside of various consumer electronic products (*e.g.*, CD and DVD players).[4] Once Tarnovsky

[3] For a complete discussion of the methods and manner in which NDS retained and/or exerted control over its hacker agents and distribution network, see Plaintiffs' RICO causes of action *infra*.

[4] Eventually, the method of payments from Menard to NDS and Tarnovsky was discovered by U.S. Customs officials who launched an investigation into Tarnovsky's activities of satellite 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

received these cash payments, Tarnovsky would write a program which would reactivate the "stinger" enabling the device to begin reprogramming a predetermined number of Access Cards until the limit was reached again. NDS, Tarnovsky, and Menard continued with this method of controlled distribution for over a year. Through this method, NDS and Tarnovsky were able to effectively "CONTROL" the piracy of Plaintiffs' Security System because they were the *only ones* capable of reprogramming or "pirating" an EchoStar Smart Card – such reprogramming being accomplished via NDS and Tarnovsky's "stinger."

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

20. As evidenced by a significant number of internet posts cited herein, the end user pirates obtaining reprogrammed EchoStar Access Cards from NDS, via Tarnovsky and Menard, became discontent with the inability of these pirated Access Cards to withstand Plaintiffs' ECMs. Specifically, with the "CONTROLLED" distribution network designed and implemented by, among others, NDS, Tarnovsky, and Menard, end users who purchased one of these reprogrammed EchoStar Access Cards had to send them back to Menard/Tarnovsky, either directly or through dealers Dawson, Quinn, Sergei, and

Tarnovsky's home without NDS's counsel being present.

Frost for "fixes" or "updates" each time Plaintiffs launched an ECM to disable the pirated Access Cards.

21. **In December 2000**, NDS, Tarnovsky and Menard, effectuated and assisted others in effectuating a wide-spread compromise of Plaintiffs' conditional access system. On these dates, using the nicknames such as "nIpPeR[5] cLaUz 00'" and "NiPpEr2000" under the direction and control of NDS, and with NDS's full knowledge and ratification, Tarnovsky posted for the first time a sequence of commands and data, along with accompanying instructional code, that provided satellite pirates around the world the "road map" and requisite instructions for: (a) the full dump of Plaintiffs' secret ROM Code; (b) the full dump of Plaintiffs' EEPROM Code and accompanying secret keys; and (c) the instructions on how to internally "hack" or access the microprocessor contained in EchoStar Access Cards thereby providing hackers the "exploit key" necessary to gain access to Plaintiffs' microprocessor and subsequently read and write to Plaintiffs' Access Cards.

22. Tarnovsky posted the foregoing on the Internet websites www.dr7.com and www.piratesden.com. As a direct and intended result of NDS/Tarnovsky's December 2000 posts, a public hack of Plaintiffs' Security System was made available, resulting in NDS's intended goal of effectuating and facilitating others in effectuating the uncontrollable and widespread compromise of Plaintiffs' Security System.

23. With this assistance, satellite pirates around the world now had all the requisite proprietary information that was once secured in Plaintiffs' microprocessor. Specifically, with these December 2000 publications, satellite

[5] The name "NiPpEr" used by Tarnovsky to post Plaintiffs' proprietary information is significant. Specifically, when Plaintiffs' Security System was developed, NagraStar's engineers concealed the term "NiPpEr" in the very heart of the secret ROM Code to serve as a unique 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.

pirates were then able to build their own card reprogrammers and, thus, were able to break free from their dependence on NDS, Tarnovsky and Menard for obtaining reprogrammed EchoStar Access Cards. As a direct and intended result of Tarnovsky's December, 2000, posts, for the first time satellite pirates around the world were able to design and implement various public (and additional private) 'hacks' of Plaintiffs' security system within a matter of months.

24. Subsequent to these December 2000 postings, NDS through Tarnovsky continued to provide technical support through updates, patches and fixes for the reprogrammed EchoStar Access Cards that had been disabled by Plaintiffs' ECMs. As a result of this information, support, and assistance, Menard and the other NDS distributors (Dawson, Quinn, Frost and Sergei) continued to: (a) unlawfully reprogram EchoStar Access Cards; (b) traffic in the unlawful sale and/or distribution of reprogrammed EchoStar Access Cards; (c) periodically update such cards after they had been disabled through one of Plaintiffs' ECMs; and (d) otherwise post or provide technical information, support services, instructions, and related assistance by and through their websites in compromising and facilitating other persons in compromising EchoStar Access Cards and the unlawful piracy and circumvention of Plaintiffs' Security System.

25. This unlawful conduct continued up to and including the following dates on which the respective pirating websites were shut down: (1) Menard – www.dr7.com – June 21, 2001; (2) Dawson –www.discountsatellite.com; www.dsscanada.com – June 19, 2003; (3) Quinn – www.hitecsat.com – June 19, 2003; (4) Sergei – www.koinvizion.com – January 28, 2001; and (5) Frost – www.newfrontiergroup.com – June 25, 2003.

26. In addition to providing the necessary technical support to maintain the modified EchoStar Access Cards distributed by NDS, Tarnovsky and Menard through Dawson, Quinn, Sergei and Frost, Tarnovsky also continued to unlawfully reprogram other EchoStar Access Cards up to and including January 9, 2001 when

federal officials arrived unannounced at his California home.

27. As a result of the conduct alleged herein, particularly the December 2000 postings by Tarnovsky with the assistance and direction of NDS, the continued reprogramming of EchoStar Access Cards by Tarnovsky up to and including January 9, 2001, and the unlawful operation of the distribution websites by Menard, Dawson, Quinn, Sergei, and Frost up to and including June 25, 2003, Plaintiffs have suffered and will continue to suffer substantial damages. Moreover, *the December 2000 postings by NDS/Tarnovsky put at risk over 7.6 million of Plaintiffs' Access Cards already distributed in the marketplace. Consequently, Step 4 of the NDS conspiracy rendered a global card-swap by Plaintiffs unavoidable.*

## II. JURISDICTION & VENUE

28. Jurisdiction and venue are proper in this court. This Court has original federal question subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338, the Communications Act of 1934, as amended, 47 U.S.C. § 605(e)(3)(A), the Digital Millennium Copyright Act, 17 U.S.C. § 1203, the Racketeer Influenced and Corrupt Organizations Act ("RICO"), and 18 U.S.C. § 1965(b). Alternatively, this Court has subject matter jurisdiction of this action under 28 U.S.C. § 1332(a)(1) by virtue of the complete diversity of citizenship of the parties in an action in which the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs. This Court also has supplemental jurisdiction, pursuant to 28 U.S.C. 1367(a), over the California state law claims asserted herein.

29. Personal jurisdiction and venue are proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b), (c), and (d), 18 U.S.C. § 1965(a), (b), and (d), and Federal Rule of Civil Procedure 4(k)(1) and (2). Pursuant to 18 U.S.C. § 1965, Plaintiffs allege that (1) Defendants have engaged in a multi-district conspiracy, (2) this Court has personal jurisdiction of at least one participant, and (3) there is no other District in which the United States District Court would have personal

jurisdiction over all the co-conspirators. In addition the Alien Venue Act, 28 U.S.C. Section 1391(d) provides that "an alien may be sued in any district." Venue is additionally proper in this District and all Defendants named herein are subject to *in personam* jurisdiction in this District because each Defendant has made repeated and substantial contacts with this judicial district by, *inter alia*, providing assistance to NDS and/or Tarnovsky in this District in serving their role in the overriding NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system. Further, venue is proper in this District because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District. Defendants have further advertised, solicited orders from and/or sent satellite pirating equipment and/or proceeds unlawfully obtained through the trafficking in satellite pirating equipment through interstate commerce to this State.

## III. PARTIES & RELATIONSHIP TO PLAINTIFFS' SUIT

30. Plaintiff NagraStar LLC ("NagraStar") is a joint venture and Colorado corporation with its principal place of business at 90 Inverness Circle East, Englewood, Colorado 80112.

31. Plaintiff EchoStar Communications Corporation ("ECC") is a Nevada corporation with its principal place of business at 9601 South Meridian Blvd., Englewood, Colorado 80112. ECC is the corporate parent of EchoStar Satellite Corporation and EchoStar Technologies Corporation, and is a fifty-percent owner of NagraStar L.L.C.

32. Plaintiff EchoStar Satellite L.L.C., ("ES") f/k/a EchoStar Satellite Corporation, is a Colorado corporation and subsidiary corporation of Plaintiff EchoStar Communications Corporation with its principal place of business at 9601 South Meridian Blvd., Englewood, Colorado 80112.

33. Plaintiff EchoStar Technologies Corporation (ETC") is a Texas corporation that is a wholly owned subsidiary of ECC. Plaintiff ETC has its

principal place of business at 90 Inverness Circle East, Englewood, Colorado 80112.

34. Defendant NDS Group, PLC ("NDS Group") is incorporated under the laws of England and Wales, with its registered address for service at One London Road, Staines, Middlesex, England TW18 4EX and its U.S. agent for service of process is Arthur Siskind c/o The News Corporation Limited, 1211 Avenue of the Americas, New York, New York. As alleged herein, NDS Group unlawfully hacked into Plaintiffs' microprocessor in its Haifa, Isreal laboratory and successfully extracted the ROM and EEPROM codes secured therein. Subsequently, NDS Group transferred these codes to NDS Americas employee Tarnovsky with instructions to use the codes to build a reprogramming device, assist in the creation and maintenance of a distribution network through which the reprogrammed cards could be sold, and provide technical support for the reprogrammed cards thereafter.

35. Defendant NDS Americas, Inc. ("NDS Americas") is a Delaware Corporation with its principal place of business in Newport Beach, California, and its registered agent for service of process is John Workman, 3501 Jamboree Road, Suite 200, Newport Beach, California. As alleged herein, NDS Americas assisted Tarnovsky in: (a) using the ROM and EEPROM codes extracted from Plaintiffs' microprocessor by NDS Group to design and build a reprogramming device and using same to modify EchoStar Access Cards up to and including January 9, 2001; (b) creating and maintaining a controlled distribution network through which reprogrammed EchoStar Access Cards could be sold, up to and including June 25, 2003; (c) providing technical support for these reprogrammed cards thereafter up to and including June 25, 2003; and (d) posting the instructional code necessary for others to hack Plaintiffs' microprocessor on the world wide web in December 2000.

36. Defendants NDS Group PLC and NDS Americas are still currently in possession of: (a) Plaintiffs' proprietary information including but not limited to

proprietary sections of Plaintiffs' ROM code, Plaintiffs' EEPROM code, and/or other proprietary information unlawfully extracted from the microprocessor embedded in EchoStar Access Cards; (b) software, hardware, Pirated EchoStar Access Cards and/or other Signal Theft Devices designed to enable users to illegally modify or alter EchoStar Access Cards and/or Plaintiffs' Security System (including, but not limited to, loaders, dead processor boot boards, glitchers, bootloaders, unloopers, emulators, printed circuit boards, programmers, integrated receivers/decoders, Audio Video Replicators "AVRs," AVR wafers, ATMEGA 128s, JTAGs, Digi-Locks, and/or other hardware and software intended for the unlawful and unauthorized modification of and/or access to EchoStar's digital satellite system) (hereinafter collectively referred to as "Circumvention or Signal Theft Devices"); and/or (c) monies or other proceeds unlawfully obtained through the sale/distribution of, or assistance or support provided in connection with, among others, Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices.

## IV. RELATIONSHIP BETWEEN DEFENDANTS AND THEIR EMPLOYEES, AGENTS, SUB-AGENTS AND CO-CONSPIRATORS

37. To clarify, Plaintiffs are not predicating the entire 5AC on any alleged "unified course of fraudulent conduct." Rather, Plaintiffs' claims are based on a multi-layered conspiratorial web consisting of corporate entities seeking to gain dominance in the CAS marketplace and individuals seeking to profit from serving their respective roles in carrying out this anticompetitive objective. Consequently, Plaintiffs' claims are based on a course of anticompetitive conduct and *not* any alleged course of "unified fraudulent conduct". As seen *infra* in the Causes of Action section, Plaintiffs are asserting both direct and indirect theories of liability against Defendants. In support of those respective theories, Plaintiffs have included

this section of the 5AC to outline the hierarchy and/or interrelatedness of these various Defendants and individuals.

**A. Direct Employment Relationship**

38. The following individuals are or were at all times relevant as stated herein, directors, officers, and/or employees acting under the direction and control of NDS Group and/or NDS Americas: (1) John Norris; (2) Reuven Hasak; (3) Chris Tarnovsky; and (4) Oliver Kommerling. All acts and/or omissions committed by the foregoing individuals, as stated herein, were: (1) required by or incident to their employment duties with NDS Group and/or NDS Americas; and/or (2) reasonably foreseeable to NDS Group and/or NDS Americas. Furthermore, all acts and/or omissions committed by the foregoing individuals, as stated herein, including compromising and/or facilitating other persons in compromising Plaintiffs' Security System benefited NDS Group and/or NDS Americas in securing an unlawful anticompetitive advantage in the CAS marketplace.

**B. Agency Relationships**

**1. Agency/Sub-Agency:**

39. The following individuals were, at all times relevant as stated herein, agents and/or sub-agents of NDS Group and/or NDS Americas acting under the direct and/or indirect control and supervision of NDS Group and/or NDS Americas, via Hasak, Norris and/or Tarnovsky, with all acts and/or omissions being committed in furtherance of NDS's ultimate goals of effectuating and/or facilitating others in effectuating the widespread compromise of Plaintiffs' Security System and ultimately eliminating Plaintiffs as competitors of NDS in the CAS marketplace:

**a. Allen Menard**

40. NDS used its hacker-employee Tarnovsky to approach and successfully solicit the assistance of Menard to facilitate NDS's overriding conspiratorial goals on the distribution side. Menard was acting at all times

relevant herein as NDS's agent and received instructions and direction from NDS Group and/or NDS Americas, via Tarnovsky. NDS Group and/or NDS Americas used NDS Americas' employee Tarnovsky to retain and exercise control over Menard and the distribution side of NDS's unlawful enterprise. With the assistance and at the direction of NDS Group and/or NDS Americas, via Tarnovsky, Menard contacted and recruited a select group of hacker individuals to be used as distributors for the unlawfully reprogrammed EchoStar Access Cards and other Signal Theft Devices being manufactured, advertised, sold, distributed, provided, and/or otherwise trafficked in by the NDS/Tarnovsky/Menard distribution network. These individuals included Dave Dawson, Sean Quinn, Andre Sergei, and Stan Frost.

41. To successfully solicit these distributors, and acting under the advice, direction, and control of NDS Group and/or NDS Americas, via Tarnovsky, Menard represented to them that: (1) NDS was behind the EchoStar hack; (2) the NDS/Tarnovsky/Menard distribution network would be protected and controlled by NDS; (3) NDS had an agreed to arrangement with Tarnovsky to facilitate the production of unlawfully reprogrammed EchoStar Access Cards and to provide subsequent software and technological support to combat ECMs launched by Plaintiffs to disable those reprogrammed EchoStar Access Cards; and (4) NDS would provide protection for the NDS/Tarnovsky/Menard distribution network from potential RCMP raids.

**b. <u>Dawson, Quinn, Sergei, and Frost</u>:**

42. As stated above, NDS Group and/or NDS Americas directed Menard, via Tarnovsky, to solicit the help of Dawson, Quinn, Sergei, and Frost to serve the role of distributors for the unlawfully reprogrammed EchoStar Access Cards and other Signal Theft Devices. In compliance with NDS's instruction, Tarnovsky and Menard established a distribution network for the unlawfully reprogrammed EchoStar Access Cards and other Signal Theft Devices in a manner that NDS could

control. Because Tarnovsky and Menard solicited the help of Dawson, Quinn, Sergei, and Frost to act on behalf of NDS and under NDS's control via Tarnovsky and Menard, Dawson, Sergei, Quinn, and Frost thereby became sub-agents of NDS.

43. In accordance with serving out their roles as distributor sub-agents in the implementing NDS's objectives, Dawson, Quinn, Sergei, and Frost facilitated the compromise of Plaintiffs' Security System by advertising, selling, distributing, providing, and/or otherwise trafficking in, among others, illegally reprogrammed EchoStar Access Cards and/or other Signal Theft Devices. The medium used for this unlawful conduct was the internet through several pirating websites. The NDS/Tarnovsky/Menard distribution network continued to operate and engage in the acts underlying Plaintiffs' claims up to and including: (1) Menard – www.dr7.com – June 21, 2001; (2) Dawson –www.discountsatellite.com; www.dsscanada.com – June 19, 2003; (3) Quinn – www.hitecsat.com – June 19, 2003; (4) Sergei – www.koinvizion.com – January 28, 2001; and (5) Frost – www.newfrontiergroup.com – June 25, 2003.

**c. Mervin Main:**

44. NDS's agent Menard additionally solicited the assistance of Mervin Main to help in establishing and operating NDS's distribution network. Upon being approached by Menard, Main agreed to assist in the NDS/Tarnovsky/Menard distribution network. And, because Menard's solicitation of Main was a foreseeable result of NDS's agency relationship with Menard, in addition to the fact that Main acted in furtherance of NDS's ultimate goals and NDS accepted the benefit of such acts, Main was not only an agent of Menard, but also the sub-agent of NDS.

C. **Agency by Ratification:**

45. Menard, Dawson, Sergei, Quinn, Frost, and Main also became NDS's agents by subsequent ratification. To be sure, NDS: (1) had full knowledge and/or was willfully ignorant of the unlawful acts engaged in by Menard, Dawson, Sergei,

Quinn, Frost, and Main in furtherance of carrying out NDS's objectives through the NDS/Tarnovsky/Menard distribution network; and (2) accepted and/or retained the benefits and commercial advantage obtained through the unlawful acts of Menard, Dawson, Sergei, Quinn, Frost, and Main. Indeed, the NDS internal documents cited and quoted from herein clearly demonstrate NDS's full awareness of the acts of each of its pirate-agents and sub-agents, as well as the direct benefit and commercial advantaged bestowed upon NDS by the unlawful acts of same.

D. **Co-Conspirators of NDS Group and NDS Americas**

46. The following individuals were at all times relevant herein acting as co-conspirators of NDS Group and/or NDS Americas in serving their role in implementing NDS's unlawful objectives of compromising and facilitating others in compromising Plaintiffs' Security System and ultimately eliminating Plaintiffs as a competitor in the CAS marketplace: (1) Norris; (2) Hasak; (3) Tarnovsky; (4) Kommerling; (5) Menard; (6) Main; (7) Dawson; (8) Quinn; (9) Sergei; and (10) Frost.

47. Each of these individuals knowingly entered into agreement with NDS Group and/or NDS Americas and/or each other to establish the NDS/Tarnovsky/Menard distribution network with the common purpose of compromising and facilitating other persons in compromising Plaintiffs' Security System by advertising, selling, distributing, providing, and/or otherwise trafficking in illegally reprogrammed EchoStar Access Cards and/or other Signal Theft Devices. In addition to their employee, agency and/or sub-agency relationships with NDS, the foregoing individuals were also acting in concert with NDS Group and/or NDS Americas as co-conspirators vis-à-vis the overriding NDS conspiracy to eliminate Plaintiffs from the CAS marketplace.

48. NDS conspired with and through their directors, officers, and/or employees (Norris, Hasak, Tarnovsky, and Kommerling) to effectuate and facilitate others in effectuating the widespread compromise of Plaintiffs' Security System

through the 2-phase process outlined in the introductory paragraphs and detailed *infra*. NDS, through, among others, Tarnovsky, conspired with Menard to assist in NDS's overall conspiracy by establishing and maintaining, with the assistance of NDS and Tarnovsky and under their direct and/or indirect control, a distribution network consistent with NDS's overall objectives. In furtherance of NDS's objectives vis-à-vis this distribution network, Menard conspired with Dawson, Sergei, Frost, Quinn, and Main to provide assistance in carrying out NDS's goals of assisting others in compromising Plaintiffs' Security System.

## V. PLAINTIFFS' & DEFENDANTS' SECURITY SYSTEMS

### A. The Components of Plaintiffs' Security System.

49. A consumer wishing to subscribe to the DISH Network must first have the necessary equipment, which consists primarily of: (1) a satellite dish antenna ("dish"); (2) an integrated receiver/decoder ("IRD," "receiver," or "set-top box"); and (3) a credit card-sized EchoStar Access Card ("Access Card").

50. EchoStar Access Cards are purchased from NagraStar and are provided by EchoStar to DISH Network subscribers for use in connection with the set-top box for the sole purpose of enabling legally authorized access to EchoStar Programming. DISH Network subscribers are not authorized to modify EchoStar Access Cards which are clearly marked as the property of EchoStar and must be returned upon request. EchoStar's ownership of its Access Cards is explained in the DISH Network's subscriber agreement:

> The Smart Card remains the property of EchoStar . . . and ***any tampering or unauthorized modification to the Smart Card is strictly prohibited and may result in, and subject you to, legal action.*** You agree to return the Smart Card 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.*** (emphasis added).

51. EchoStar Access Cards are essential to the operation of the DISH

Network. An EchoStar Access Card is, in and of itself, a secure computer which contains a microprocessor unit. The microprocessor unit stores data and encryption technology and performs various computing and customer entitlement functions enabling the Access Card and set-top box to communicate with one another resulting in the unscrambling of EchoStar's satellite signal enabling authorized subscribers access to EchoStar's DISH Network Programming,

52. The microprocessor unit is supported by two segments of memory: (1) Read-Only-Memory ("ROM"); and (2) Electronically Erasable Programmable Read-Only-Memory ("EEPROM"). Generally, the ROM Code segment contains the intimate knowledge and information about Plaintiffs' Security System and how it works, whereas the EEPROM Code segment contains secret keys enabling the decryption of EchoStar's satellite signal. In order for a pirate to fully develop a "hack" for Plaintiffs' Security System, a pirate must have the detailed information and intimate knowledge of the code memory contained in both the ROM Code segment and the EEPROM Code segment of an EchoStar Access Card.

53. The ROM Code segment provides detailed instructions and commands to EchoStar Access Cards and set-top boxes in the normal operation of Plaintiffs' Security System. The "Nagra ROM Code" is the quintessential component of Plaintiffs' Security System and access to the detailed information and intimate knowledge contained therein is mandatory for a pirate trying to unlock the safe to Plaintiffs' secrets controlling Plaintiffs' Security System.

54. The EEPROM Code segment stores data and can potentially store code commands that have been written to EchoStar Access Cards which remain even if the Access Card does not have power, but which can be erased and modified. The EEPROM Code contains data that the ROM Code segment reads from in performing its calculation and operation functions. The EEPROM Code segment contains secret "transmission" keys (sometimes called "decrypt keys NN" in illegal Internet posts) and secret "pairing" keys (sometimes called "secret box key" in

illegal Internet posts). The "pairing keys" are used to encrypt and decrypt the communications between the EchoStar Access Card and the set-top box.

55. EchoStar frequently communicates with the microprocessor chip on the Access Card by sending and receiving information which is routinely updated. The information transmitted to and temporarily stored on the Access Card microprocessor and in related memory, includes the most recent software code related to the functioning of certain portions of Plaintiffs' Security System.

56. Plaintiffs' Security System effectively controls access to copyrighted works included in DISH Network programming. In addition, the Security System ensures that the protection afforded to this copyrighted material, such as limitations on the dissemination and use in accordance with EchoStar's contractual agreements with content providers, is preserved. Plaintiffs also have valid copyrights and associated protection in software and/or codes contained in: (a) EchoStar Access Cards; (b) EchoStar Receivers; and (c) other aspects of Plaintiffs' CAS.

### B. NDS Was Fully Compromised as Early as 1995 and Was Losing Credibility in the Conditional Access System Market Place.

57. Three companies manufacture the majority of "conditional access systems" for the Direct-to-Home Broadcast Satellite ("DBS") industry world-wide. Two of those companies are NDS and its related companies, and NagraStar and its related companies, including the Kudelski Group.

58. NDS supplies the conditional access system used by DirecTV, a DBS company in the United States and direct competitor of Plaintiff EchoStar.

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

60. Upon information and belief, after its Security System had been fully compromised and NDS became aware of its inferior technology and its inability to maintain the integrity of its Security System, NDS made a conscious decision to hire and "control" all of the most well-known, or "best" satellite pirates and hackers. Using these hackers, NDS could then control the piracy of its technology.

61. On or about February 1997, NDS superficially attempted to "remedy" certain problems plaguing their Security System by releasing a second-generation smart card, known in the industry as the "P2" card. NDS convinced DirecTV to initiate a "swap out" program, whereby all first generation cards, the NDS "P1" cards, were exchanged for NDS "P2" cards at DirecTV's expense – costing millions of dollars. On or about July 7, 1997, the swap out was complete and the "P1" system was shut down completely.

62. By the end of August 1997, however, the new "P2" system had been successfully hacked, leaving DirecTV with nothing to show for its expensive card swap. Once again, DirecTV was left with a compromised NDS conditional access system.

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

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

64. In the summer of 1998, DirecTV put out a Request for Information because they were considering replacing NDS as their Security System provider, due to the problems DirecTV was having with the piracy and hacking of NDS's inferior conditional access technology.

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

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

## VI. DEFENDANTS' CONCERTED OR OTHERWISE INTERRELATED UNLAWFUL CONDUCT[6]

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

67. By at least September 26, 1997, NDS had full knowledge that their technology was being widely compromised and that their continued viability in the CAS arena was in jeopardy. This fact is supported by an internal NDS memorandum on this date titled "Main Story" which was submitted to Hasak.

68. By at least October 6, 1997, NDS was employing both Tarnovsky and Kommerling in an effort to control the compromise of NDS's encryption technology. On or about this same date, NDS, Hasak and Norris received an internal memorandum from NDS employee Segoly discussing Tarnovsky and the control NDS retained over Tarnovsky's interaction with other satellite pirates. In this same memorandum, Segoly (a) acknowledges the high level of hacking

[6] Plaintiffs' allegations as to themselves are based upon personal knowledge. Plaintiffs' allegations as to Defendants are based upon information and belief, documents Plaintiffs have reviewed, interviews conducted by Plaintiffs and sworn affidavit or declaration testimony attached to Plaintiffs' 5AC and hereby incorporated.

activities that Tarnovsky was capable of engaging in; (b) references NDS's employment of Kommerling (without Tarnovsky's knowledge); and (c) inquires into the possible recruitment by NDS of another hacker, Deiter Scheel.

69. By at least October 21, 1997, NDS's internal memorandums openly acknowledged and discussed NDS's ability to control Tarnovsky's interaction and participation within the pirating community.

70. By at least October 22, 1997, NDS had successfully solicited and began employing Luyando to assist in controlling the piracy of NDS's technology. In an internal NDS memorandum acknowledging this issue, it goes on to acknowledge that NDS and Norris were concealing their employment relationship with Kommerling from DirecTV. The memo goes on to illustrate NDS's ability to control its hacker-employees by, *inter alia*, controlling their ability to travel together and participate in the pirating community. Importantly, this internal NDS memorandum evinces the efforts NDS and Kommerling went through to conceal their pirating activities by, *inter alia*, shipping Kommerling's computer linking NDS to its pirating activity in two separate parts, by different couriers, to different addresses in Germany.

71. On or about November 10, 1997, Norris sent an NDS Letter to another NDS employee advising that Tarnovsky had successfully hacked a compulator chip and exposed its "heart".

72. On or about November 13, 1997, is the first reference that Larry Rissler, Vice President of Signal Integrity for DirecTV, could locate in his notes to "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 [Norris] had recruited Tarnovsky to work as a consultant for NDS, and that Norris had moved Tarnovsky to California."[7]

[7] In contrast, Norris was not so forthright with U.S. 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

73. In or about March 1999, Norris and Tarnovsky attended the SBCA show in Las Vegas, Nevada. Norris introduced Tarnovsky under the NDS alias "Mike George," and claimed Tarnovsky was his nephew.

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

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

75. On or about May 31, 1999, an NDS Letter was sent from Yehonatan Shiloh from NDS Technologies Israel, Ltd. to the Israeli Embassy acknowledging that Defendant Plamen Donev was employed by NDS as an alleged "Director and Advisor for Technical Design and Research."

76. On or about June 18, 1999, Hasak received an internal letter from

---

officials that: (a) the equipment in Tarnovsky's home – which included various pirating devices such as a card emulator for use in reprogramming EchoStar Access Cards, among other unlawful purposes – was property of NDS; (b) Tarnovsky was an NDS employee for years; and (c) the U.S. Customs officials were not to search Tarnovsky's home without a search warrant.

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

[9] Rupert Murdoch's News Corp. is the parent company of NDS.

Adams acknowledging NDS's recruitment of various satellite pirates (including Kommerling and Tarnovsky) in an effort to control the piracy of NDS's technology. This letter states in relevant part:

> *So if a risk existed what were we to do. With Risks we normally think of: AVOIDANCE, REMOVE, CONTROL*
>
> *We could avoid the risk by not introducing P3. We could remove the risk by introducing an un-hackable card. So, we are left with CONTROL.*
>
> *We decided that the best control was to control the perpetrators [pirates and hackers]. To control we decided to recruit, to neutralise. The twin advantages of doing this were:*
>
> *1. to stop them actively hacking P3 on behalf of the Canadians*
> *2. to learn from the two recruits (referring to Pluto [Plamen Donev] and Vesco [Vesselin Nedeltchev]), their methods, and preventative measures.*
>
> *With the benefit of experience over the next six months you and I will be able to talk very convincingly about the cost benefit of our recruitment.*
>
> *The one hostage that we carry into all these deliberations is the weaknesses in our [NDS's] technology [Access Cards]. I have not told you before as i assume you already know the same as me. Yossi admits that our cards are even more vulnerable to attack than anyone realised before. Glitching is practically a magic key to access our cards. . . .*
>
> *So given that the technology can be hacked very quickly what do we do. Do we abandon recruitment [of other satellite pirates and hackers] and leave everything to ECM's [electronic countermeasures to fight piracy] in which case we will lose our customers [DirecTV] in a short space of time. Or, do we continue to recruit [hackers]. This gives us time to get the technology correct. Having the enemy [hackers and pirates] on our side removes the complacency element and makes the improvement of our technology a geometric progression.*

> *. . . .What we need is support. In the main that is money, money, money.*
>
> *Without a realistic budget we cannot recruit the top hackers. They know what they can get from the pirates. . . . . We need to control these guys, to pay them well, and get benefit from them.*
>
> *... JOD was heavily involved in the DTV negotiations. He thinks we will lose them soon. We will lose them quicker if P3 if hacked. This must be a major concern.*[10]

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

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

> *I think we should reflect on what the objective is, either, to get the programme, or, to run a complex operation. I feel sure that, for understandable reasons, the possibility of looking at alternatives is being passed over. Why not for example, let Alex [Kommerling] and Mike [Tarnovsky] run together on this one. Why separate them? I am prepared to let JN [John Norris] run the operation.*
>
> *. . . For some time there has been speculation about Kommerling and the fact that he is no longer acting with the pirates. His withdrawal from the USA scene will serve to confirm the suspicions. He is*

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

*suppose to be a pirate and should therefore act like one. . . . In one simple move we would get the operation moving and protect Kommerling from exposure....he [Jan Saggiori] knows that Kommerling is with NDS.*

78. On or about December 1, 1997, an NDS Memorandum entitled "Operations Security Group" from was circulated to Hasak, Segoly, Adams, and Norris acknowledging NDS's placement of Tarnovsky into Ron Ereiser's pirate organization with NDS's full support. On or about that same day Norris sent Adams a letter advising that Tarnovsky had concerns about NDS protecting him from his unlawful piracy conduct.

79. In November of 1998, NDS internal memoranda express concern over their future budget to employ its hacker-employees due to a cost-cutting reform and suggesting another hack of its technology to retain the need for their budget.

80. NDS internal correspondence in December of 1998 acknowledge that (a) NDS set up the company ADSR with Kommerling to give Kommerling "a business face that will explain to others what he is doing;" (b) alleging that NDS/Kommerling was going to hack the Irdeto (a competitor) card; (c) and requesting "some official [Access] cards from each of the system[s]" to make the hack "effective and untraceable."

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

**1. Step 1: With the Assistance of Kommerling, NDS Built a Sophisticated Laboratory in Haifa, Israel, Where NDS Hacked Plaintiffs' Access Card and Extracted Plaintiffs' Secret and Proprietary ROM and EEPROM Codes.**

81. Plaintiffs' secret and proprietary ROM and EEPROM codes are embedded and secured within the microprocessor affixed to EchoStar Access

Cards. To extract, or "dump" these protected codes, requires a highly sophisticated laboratory, probing and extracting devices, and skilled engineers. At the time NDS hacked into Plaintiffs' microprocessor, there were only 6 of these facilities in the world. NDS owned and operated one such facility that was built by NDS with the help of Kommerling.

82. Kommerling testified in the *Canal+ v. NDS* case that NDS engineers at NDS's Matam Centre research facility in Haifa, Israel used the methods and techniques described in "Design Principles for Tamper Resistant Smartcards" (written by Kommerling and Markus Kuhn) to attack Canal+'s Access Card. Plaintiffs are informed and believe that NDS used this same procedure to physically extract Plaintiffs' ROM and EEPROM Codes embedded in EchoStar Access Cards.

83. Plaintiffs are informed and believe that NDS Matam engineers, recruited and trained by Kommerling, also disassembled and analyzed the extracted Codes from EchoStar Access Cards and explored methods to circumvent the security measures contained within EchoStar Access Cards. Once NDS obtained the encryption technology and related software code from the microprocessor, they replicated and modified the encryption and other software to interfere with the communication between the Access Card microprocessor and the Receiver that, in the ordinary course of its operation, authenticates which DISH Network Programming services legitimate subscribers are entitled to view.

**2. <u>Step 2:</u> NDS Provided their Hack Methodology to a Pirate Engineer Capable of Reprogramming Access Cards.**

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

84. Once NDS had successfully extracted Plaintiffs' secret and proprietary ROM and EEPROM Codes, they were transferred via Hasak and Norris, to

Tarnovsky along with specific instructions for Tarnovsky to use these Codes to (a) design, manufacture, and provide Menard with a device capable of reprogramming EchoStar Access Cards; (b) assist Menard in establishing and supporting a controlled distribution network for the pirated EchoStar Access cards; (c) provide technical information and support to Menard relating to EchoStar Access Cards and Plaintiffs' Security System and Codes; and (d) publically disseminate the hack methodology for Plaintiffs' Security System by publishing same on the Internet.

85. Tarnovsky was a well-known and technically competent satellite hacker/computer engineer. NDS was fully aware of Tarnovsky's hacking and reprogramming abilities when they recruited him to become an NDS employee. And, using his hacking/reprogramming abilities, combined with the support and assistance of NDS Group PLC, and NDS Americas, Tarnovsky was able to (a) use Plaintiffs' ROM and EEPROM Codes provided to him by NDS to develop an understanding of Plaintiffs' Security System; (b) with the assistance of NDS, use Plaintiffs' ROM and EEPROM Codes to design and develop hardware (*e.g.*, the stinger) that NDS, Tarnovsky, and Menard used to later reprogram Plaintiffs' Access Cards; (c) write software codes and programs to counteract Plaintiffs' ECMs; and (d) ultimately, on December 21 and 24, 2000 publically disseminate Plaintiffs' proprietary information and codes and a method to hack Plaintiffs' Security System.

**b. NDS Approached Others to Facilitate in the Proliferation of Plaintiffs' Security System**

86. Plaintiffs are informed and believe that, prior to obtaining the help of Tarnovsky, Menard, and the distributors, NDS considered other methods of disseminating Plaintiffs' Codes and unlawful software support information necessary to accomplish the wide-spread compromise of Plaintiffs' CAS. As stated in the sworn affidavit testimony of Martin Paul Stewart (f/k/a Martin "Marty" Mullen) attached and incorporated, he states as follows: (a) August 1997 he was

approached by NDS employee Kommerling and informed that he would soon be in possession of EchoStar's ROM code that was being extracted in Europe; (b) February 1998 Kommerling contacted him again to advise that EchoStar's code had been extracted and Luyando would follow-up with Mullen about the possibility of purchasing the hack; (c) Luyando contacted him in early March 1998 and arranged a meeting with him that took place March 13, 1998 at the Hilton hotel in Windsor, Ontario where Luyando stated that he had NDS's authority to negotiate the purchase of the EchoStar hack. (Mullen Affidavit at ¶¶ 16, 21, 22, 23 and 26.)

**c. NDS and Tarnovsky Designed and Built the "Stinger" that NDS, Tarnovsky, and Menard Used to Control and Monopolize the Sales and Distribution of the unlawfully reprogrammed Access Cards over the Internet.**

87. In or about 1999, Menard became the first person to possess a device that could reprogram EchoStar Access Cards enabling persons to access the DISH Network's Programming without authorization. With the assistance of NDS, Tarnovsky was able to develop, design and create this reprogrammer which he coined the "stinger." NDS then provided Menard with the "stinger" via Tarnovsky.

88. Menard was the only person to possess such a device for approximately a year and a half, or from 1999 until early 2001,[11] and thus, with the assistance of Tarnovsky and NDS, was the only person (besides NDS) who had the ability to reprogram, alter, or modify EchoStar Access Cards enabling unauthorized access to DISH Network's Programming.

[11] As a result of Tarnovsky's December 2000 postings, satellite pirates and software engineers around the world were then able to design and build their own card reprogrammers thereby exacerbating the piracy of Plaintiffs' satellite television transmission signal.

**3. Step 3: NDS, Tarnovsky, Menard and others Conspired to Place Pirated EchoStar Access Cards into the Black Market in a "Controlled" Manner and to Provide Technical Support for Same.**

**a. NDS, through its Employees/Agents Tarnovsky Menard, Created a Distribution Network for Illegally Altered Access Cards and Other Circumvention Devices Designed to Hack Plaintiffs' Security System.**

89. Through Tarnovsky, NDS successfully solicited the assistance of Menard to serve as NDS/Tarnovsky's agent in establishing a distribution network for the pirated EchoStar Access Cards reprogrammed by NDS through Tarnovsky's "stinger" and the assistance of Menard.

90. Menard was acting at all times relevant herein as NDS's agent and received instructions and direction from NDS via NDS employee Tarnovsky. NDS used its employee Tarnovsky to retain and/or exercise control over Menard and the distribution side of NDS's unlawful enterprise. With the assistance and at the direction of NDS, via Tarnovsky, Menard contacted and recruited a select group of individuals to be used as distributors for the unlawfully reprogrammed EchoStar Access Cards and other Circumvention or Signal Theft Devices being manufactured, produced, and distributed by NDS, Tarnovsky, and Menard. These individuals included: Dawson, Quinn, Sergei, and Frost.

91. To solicit these individual distributors, Menard, under the advice of NDS via Tarnovsky, represented to them that: (1) NDS was behind the EchoStar hack; (2) the Tarnovsky/Menard distribution model would be protected and controlled by NDS; (3) NDS had an arrangement with Tarnovsky to facilitate the production of unlawfully reprogrammed EchoStar Access Cards and provide subsequent software and technological support to combat ECM's launched by Plaintiffs to disable the pirated Access Cards; and (4) NDS would protect this

distribution network from potential RCMP raids.

92. With the assistance of NDS through Tarnovsky, Menard produced altered Access Cards using a machine known as a Reprogrammer to place the Access Card microprocessor in a mode that permits reprogramming. NDS provided Menard this initial reprogrammer via Tarnovsky. With the assistance of NDS, Tarnovsky was able to develop, design and create this reprogrammer which he coined, the "stinger." Menard then loaded the modified software described above, containing programs, information, codes, or commands onto the Access Card, which when re-programmed in this fashion permits access to DISH Network programming services by unauthorized users. None of this would have been possible without NDS initially cracking the Security System and providing the proprietary information to Menard through Tarnovsky. Tarnovsky was directed by NDS to provide the information to Menard.

93. From 1999 to at least June 25, 2003, NDS through Tarnovsky and Menard, used Dawson, Quinn, Sergei and Frost, and their respective websites, to advertise, sale, distribute and otherwise traffick in unlawfully altered EchoStar access cards that were reprogrammed by NDS's "stinger" through Tarnovsky and Menard.

94. From 1999 to at least June 25, 2003, NDS, by and through Tarnovsky and Menard, provided "updates," "patches," "fixes," and/or other technical support for unlawfully reprogrammed EchoStar Access Cards. This assistance and support consisted of, *inter alia,* (a) instructional or informational postings on various hacker websites including those operated by Dawson, Quinn, Sergei and Frost, to update, patch, fix or otherwise repair the reprogrammed cards which were disabled through Plaintiffs' ECMs; and (b) the actual reprogramming of said cards by Tarnovsky and/or Menard after same had become disabled.

95. As stated, the distributors engaged in the acts complained of through their respective websites including but not limited to: (1)

www.discountsatellite.com and www.DSScanada.com ("Discount Satellite"), owned and operated by Dawson; (2) www.koinvizion.com ("Koinvizion"), owned and operated by Sergei; (3) www.hitecsat.com ("Hi-Tec Satellite"), owned and operated by Quinn; (4) www.thenewfrontiergroup.com a/k/a the "Blazer Group," owned and operated by Stanley Frost; and (5) www.dr7.com, operated by Menard with the assistance Main.

96. Advertisements and "links" to these retail outlet sites were directly placed directly on Menard's website, www.dr7.com. Menard's website also maintained chat forums and message boards where other pirates and hackers could discuss and share information about the theft of DISH Network programming services and the alteration and modification of 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 to facilitate such theft.

97. Through the foregoing websites, up to and including June 25, 2003, Defendants, and those acting in concert with them, as a direct result of NDS's actions of providing Tarnovsky and Menard with the information necessary to alter Access Cards on a large scale, offered:

a. to sell Pirated 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 that permit unauthorized access to DISH Network programming services;

b. to perform the service (for a fee) of altering EchoStar Access Cards for members of the public who submit the EchoStar Access Cards through the mail;

c. to purchase EchoStar Access Cards from members of the public, presumably to permit alteration and resale of the Pirated EchoStar Access Cards for unauthorized access to DISH Network programming services; and

d. to exchange several deactivated EchoStar Access Cards submitted by members of the public for a Pirated EchoStar Access Card that would provide unauthorized access to DISH Network programming services.

98. Further illustrating the foregoing, on or about May 1999, DirecTV raided Scullion's house in Riguad, Quebec, Canada. Jim Whalen, a retired FBI Agent employed by DirecTV was on the raid. Whalen observed a handwritten note by Scullion and videotaped it and later had it transcribed. In relevant part, the note states that Menard admitted to Scullion that Tarnovsky's participation in the EchoStar hack was done at the request of NDS and that Tarnovsky had their sanction and protection concerning same.

99. As evidenced by the Scullion Declaraion attached hereto and hereby incorporated, Menard openly acknowledged that: (1) he and Tarnovsky were working for, and under the direction of NDS in establishing and maintaining the distribution network; and (2) he, Tarnovsky and the distributors had the support and protection of NDS in carrying out their unlawful activities. (Scullion Declaration ¶¶ 11, 17.)

**4. <u>Step 4:</u> NDS Sought to Eliminate Plaintiffs from the CAS Marketplace.**

100. In response to the Pirated EchoStar Access Cards being distributed by NDS through Tarnovsky, Menard, and the distribution network, Plaintiffs began launching ECMs in an effort to detect and disable these unauthorized EchoStar Access Cards.

101. NDS initially labored to counteract Plaintiffs' ECMs. Specifically, NDS, either directly or indirectly through Tarnovsky, developed additional hardware and software to be distributed via Menard which would protect or "repair" the Pirated EchoStar Access Cards attacked by Plaintiffs' ECMs. NDS, either directly or indirectly through Tarnovsky and Menard, also distributed

software codes and "fixes" via the Internet that were used to circumvent Plaintiffs' ECMs.

102. From late 1999 up to and including late December 2000 and beyond (including posts on the dealer's websites owned, operated, and/or maintained by Menard, Frost, Quinn, Sergei and Dawson up to and including June 25, 2003), NDS via Tarnovsky, provided continual technical support in the form of "patches," "fixes," software "updates," and instructional codes and/or commands to combat and/or guard against ECMs launched by Plaintiffs to disable and/or render inoperable unlawfully reprogrammed Access Cards and other Signal Theft Devices.

103. In December 2000, NDS, by and through Tarnovsky and Menard, published the necessary instructional codes and related technical information to access Plaintiffs' microprocessor and read/write to same resulting in a wide-spread and uncontrollable public compromise of Plaintiffs' Security System.

104. Specifically, on or about December 21, 2000, Tarnovsky, using the alias "nIpPeR cLaUz 00'" published a file on Menard's dr7.com website which included the hack methodology (or "recipe") that Defendants developed for EchoStar's security system and stated the following: "***there will be no boxes anymore! There will be no more fights amoungst us. Learn from this and prosper. Works across the world! Do the following: get atr, wait 500ms to ensure card is idle. Send this packet to 288-02 or equivalent ROM 3 nagra cam! Rx 4+4096 bytes and you have entire eeprom. Send this, then rx 4 bytes + 4096 bytes of eeprom***."

105. This December 21, 2000 publication by Tarnovsky on the Internet was the critical moment when the keys to Plaintiffs' safe of proprietary information contained in its Access Cards and Security System were given to the world. In this publication, NDS via Tarnovsky provided the hacker community for the first time a sequence of commands and data, along with accompanying instructional code, that provided satellite pirates around the world the "road map" and requisite instructions