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

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

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

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

ECHOSTAR SATELLITE CORPORATION, ECHOSTAR COMMUNICATIONS CORPORATION, ECHOSTAR TECHNOLOGIES CORPORATION, AND NAGRASTAR L.L.C.

Plaintiffs,

v.

NDS GROUP PLC, NDS AMERICAS, INC., JOHN NORRIS, REUVEN HASAK, OLIVER KOMMERLING, JOHN LUYANDO, PLAMEN DONEV, VESSELINE NEDELTCHEV, CHRISTOPHER TARNOVSKY, ALLEN MENARD, LINDA WILSON, MERVIN MAIN, DAVE DAWSON, SHAWN QUINN, ANDRE SERGEI,

No. SA CV 03-950 DOC(ANx)

PLAINTIFFS' THIRD 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);**

Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(e)(4);

TODD DALE, STANLEY FROST, GEORGE TARNOVSKY, BRIAN SOMMERFIELD, ED BRUCE, "BEAVIS," "JAZZERCZ," "STUNTGUY," and JOHN DOES 1 – 100,

Defendants.

5) **Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)(a);**

6) **Violation of the Lanham Act, 15 U.S.C. § 1114;**

7) **Violation of the Lanham Act, 15 U.S.C. § 1125(a);**

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

9) **Violation of RICO Statute, 18 U.S.C. § 1962(d)**

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

11) **Violation of California Penal Code § 593d(b);**

12) **Violation of California Penal Code § 593d(c);**

13) **Violation of California Penal Code § 593e(a);**

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

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

16) **Tortious Interference with Contractual Relations;**

17) **Tortious Interference with Prospective Contractual Relations/Economic Advantage;**

18) **Unjust Enrichment;**

19) **Conversion;**

20) **Breach of Contract;**

21) **Civil Conspiracy/Joint Contribution.**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

PAGE

Plaintiffs EchoStar Communications Corporation, EchoStar Satellite L.L.C. f/k/a EchoStar Satellite Corporation, and EchoStar Technologies Corporation (collectively "EchoStar"), and NagraStar L.L.C. ("NagraStar") (collectively "Plaintiffs") file their Third Amended Complaint ("TAC") against the above named Defendants and state as follows:

I. INTRODUCTION & NATURE OF THE CASE

1. Plaintiff 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. As part of its business, EchoStar uses high-powered satellites to broadcast, among other things, 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, in part, 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"). Among other things, the 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 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[1] of its conditional access system, the real and immediate threat

[1] September 26, 1997, NDS Memorandum Report to Hasak stating "At present I think we are on 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

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.[2]

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.

---

of it...We have introduced control. The question is whether the control is camouflaging the weaknesses in our technology. My fear is that it is....At present we are not gaining most of the new projects. How long before we actually lose one to a competitor. Our jobs are on the line. Maybe not yet but we are vulnerable." June 18, 1999 NDS Letter to Hasak from Adams stating "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."

[2] December 1998 NDS Letter from Ray Adams to Hasak stating "It should be a simple task for one of our techies to prove that the Australian 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."

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.[3] 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, Oliver Kommerling, Plamen Donev, Vesseline Nedeltchev, Jan Saggiori, Dieter Scheel, and John Luyando. 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. With this "control" over the hackers, NDS was also able to gain the ability to put economic leverage on its clients. Specifically, NDS could instruct, assist, and/or otherwise facilitate their hacker employees in pirating a client's CAS. Once compromised, NDS could offer the client – **for a fee** – an Electronic Counter Measure ("ECM") that would combat a hack which, unbeknownst to the client, 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

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

world – NDS owns one of them in Haifa, Israel, which was designed and built by NDS with the assistance of Kommerling[4] 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. This was not the first time NDS engaged in this unlawful conduct.[5] On April 9, 2002, NDS employee/agent Kommerling provided sworn testimony in another suit[6] brought by Canal+ against NDS for anticompetitive conduct similar to the acts alleged herein. In his 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

[4] 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.

[5] April 30, 1999, NDS Letter from Ray Adams to Hasak referencing a meeting that Kommerling had with Canal+, wherein Kommerling was asked about the DR7 [Menard] Hack release. Kommerling was asked if he could do a hack of the IRDeto system in Arabia on PANAM SAT channel ART 1, however, unbeknownst to Canal+, the hack of IRDeto was already in NDS's possession. "JR wants Alex [Kommerling] to hack the system but at the same time to provide a 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.

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.[7] To accomplish this, NDS, via Tarnovsky, enlisted the assistance of Allen Menard[8] 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, Shawn Quinn, Andre Sergei, Todd Dale, and Stanley Frost, among others – NDS, Tarnovsky, and Menard could "control" the

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

[8] April 16, 1999 NDS Letter from Ray Adams to Hasak concerning, among other things, a piracy 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]."

number of pirated EchoStar Access Cards that were being distributed to the pirating public.

17. In addition to Dawson, Quinn, Sergei, Dale, and Frost, among others, Menard and Tarnovsky approached other individuals to help facilitate and promote the overriding NDS conspiracy. Specifically, 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.[9] 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).[10] Once Tarnovsky received these cash payments, Tarnovsky would write a program which would reactivate the "stinger" enabling the device to begin reprogramming a

[9] 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*.

[10] 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 Tarnovsky's home without NDS's counsel being present.

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 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 chat 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, Dale, and Frost, among others, for "fixes" or "updates" each time Plaintiffs launched an ECM to disable the pirated Access Cards. Eventually, the NDS, Tarnovsky, and Menard "CONTROLLED" distribution network was unable to effectively keep up

with the ECMs employed by Plaintiffs to disable the pirated EchoStar Access Cards being reprogrammed, marketed and distributed by Defendants Tarnovsky, Menard, Dawson, Quinn, Dale, Frost, Sergei, Dale, Bruce and Sommerfield. Additionally, as NDS, Tarnovsky, and Menard had already made an obscene amount of illegal revenue through the trafficking of these pirated Access Cards, NDS "pulled the trigger" on Step 4 of their overriding conspiracy to destroy Plaintiffs as a competitor in the DBS and CAS marketplaces.

21. Indeed, **on December 23 and 24, 2000**, NDS, Tarnovsky and Menard, for the first time, effectuated and assisted others in effectuating a wide-spread compromise of Plaintiffs' conditional access system. On these dates, using the nickname "nIpPeR[11] cLaUz 00'," among others, under the direction and control of NDS, and with NDS's full knowledge and ratification, Tarnovsky posted for the first time a sequence of events 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 Plaintiffs' microprocessor thereby granting the ability to 'read' and 'write' to Plaintiffs' Access Cards. In essence, Tarnovsky's December 23 and 24, 2000, postings provided hackers, for the first time, with the 'Exploit key' or method necessary to gain access to Plaintiffs' microprocessor and subsequently read and write to Plaintiffs' Access Cards. Tarnovsky posted the foregoing, which was illegally obtained by NDS in its Haifa, Israel lab and sent to Tarnovsky in California, via Hasak and Norris, with the specific instructions to effectuate and assist others in effectuating a wide-spread

[11] 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.

compromise of Plaintiffs' conditional access system, on the Internet website www.piratesden.com. And, as a direct and immediate result of NDS/Tarnovsky's December 2000 posts, a public hack of Plaintiffs' Security System was made available within days resulting in NDS's intended goal of effectuating and facilitating others in effectuating the uncontrollable and widespread compromise of Plaintiffs' Security System. With this assistance, satellite pirates around the world now had all the requisite proprietary information that was once secured in Plaintiffs' microprocessor. Specifically, with this December 23 and 24, 2000, assistance by NDS, Tarnovsky, and Menard, among others, satellite 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, among others, for obtaining reprogrammed EchoStar Access Cards. As a direct and intended result of Tarnovsky's December 23 and 24, 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. Consequently, NDS's goal of effectuating and assisting others in effectuating the wide-spread compromise of Plaintiffs' Security System began to rapidly materialize.

22. As a result of the conduct alleged herein, particularly the December 23 and 24, 2000, postings by Tarnovsky with the assistance and direction of NDS, Plaintiffs have suffered and will continue to suffer substantial damages. Particularly, *the December 23 and 24, 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.*

23. The anticompetitive method in which NDS conspired to, and did, launch an invasive attack on Plaintiffs' conditional access system and subsequently designed and implemented the wide-spread compromise of Plaintiffs' Security

System shocks the conscience of modern-day capitalism and basic tenets of lawful competition. The unlawful acts engaged in by Defendants in furtherance of the overriding NDS conspiracy form the backdrop of an unprecedented level of corporate espionage and are illustrative of nothing less than high risk corporate financed organized crime. The time has finally come for NDS to answer for its actions.

II. JURISDICTION & VENUE

24. 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 Electronic Communications Privacy Act ("Federal Wiretap Laws"), 18 U.S.C. §2520(a), the Lanham Trademark Act, 15 U.S.C. §§ 1051 *et seq.*, the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1965(b), and 15 U.S.C. § 1121(a). 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.

25. 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. 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.

26. Defendants Menard, Dawson, Dale, Quinn, Frost, Sergei, Bruce and Sommerfield are additionally subject to the Court *in personam* jurisdiction as a direct result of their operation, participation and maintenance of their websites including www.dr7.com; www.thenewfrontier.com; www.discountsatellite.com; www.dsscanada.com; www.hitecsatellite.com; www.hitecsat.com; and www.koinvision.com. Through the aforementioned websites, which were accessible within the State of California, among others, these Defendants advertised, marketed, promoted, sold, trafficked in and supported illegally altered, modified, pirated and reprogrammed EchoStar Access Cards and other circumvention devices to individuals and entities within the State of California, among others.

III. PARTIES & RELATIONSHIP TO PLAINTIFFS' SUIT

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

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

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

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

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

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

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

37. Defendant Reuven Hasak a/k/a "RH" ("Hasak") is an individual and citizen of Israel, residing in Israel. During all times relevant as stated herein, Hasak was either: (a) working for, at the direction of, and under the direct and/or

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

38. Hasak is Head of Security for NDS in Haifa, Israel. Hasak is a former deputy of the Shin Bet, the Israeli internal security service. Hasak is fully aware of NDS's problems associated with the conditional access technology of its security system in that it is insecure and easily hacked. Hasak is fully aware of NDS's efforts and plan to "CONTROL" satellite piracy by recruiting and hiring known satellite pirates to work as double agents on NDS assignments. Hasak, Norris, Adams, Gutman, and Segoli conspired with the satellite pirates NDS hired including, but not limited to, Tarnovsky, Kommerling, Donev, and Nedeltchev, among others, to (1) illegally obtain and extract NDS's competitors' ROM codes and keys, (2) illegally design, manufacture, and distribute signal theft devices used to circumvent the technological encryption measures contained in satellite providers' access cards for the unauthorized reception of satellite television programming, (3) illegally provide software, information, and technical support services relating to satellite providers' access cards and other circumvention or signal theft devices designed to enable users to illegally modify satellite providers' access cards, and (4) illegally facilitate the wide-spread distribution of NDS's competitors' proprietary codes and keys by publishing same on the Internet.

39. Plaintiffs are informed and believe that Hasak gave both the full Canal+ ROM Code, as with Plaintiffs' ROM Code, to Norris with specific instructions to give to Tarnovsky for the use and purpose to (1) design, manufacture, and distribute to Menard signal theft devices used to circumvent the

technological encryption measures contained in Canal+'s access cards, as with Plaintiffs' Access Cards, (2) provide software, information, and technical support services relating to Canal+'s ROM Code and access cards, as with Plaintiffs' ROM Code and Access Cards, and (3) facilitate the wide-spread distribution on the Internet of the Canal+ ROM code, as with Plaintiffs' ROM Code. Tarnovsky followed Hasak's and Norris's instructions of designing, manufacturing, and distributing to Menard such signal theft devices, providing software, information, and technical support services related to same, and posting both (1) Canal+'s ROM code on www.dr7.com on March 26, 1999, and (2) Plaintiffs' ROM Code on www.piratesden.com on December 24, 2000, which Tarnovsky states this is the "full ECHO ROM dump" and it's "DR7's [Menard's] code."

40. Hasak was also aware of the real and credible threat to NDS, by its competitor NagraVision, for providing DirecTV's conditional access system should NDS be unable to compete due to its security system being insecure and easily hacked. Plaintiffs are informed and believe that it was the perceived threat to NDS's business by NagraStar that caused NDS to (1) illegally obtain and extract Nagra's ROM code and keys, (2) design, manufacture, and distribute Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices for the unauthorized reception of EchoStar's DISH Network satellite television programming, (3) provide software, information, and technical support services relating to Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices, and (4) facilitate the widespread distribution of the Nagra ROM code on the Internet. The mission of NDS's international conspiracy was initiated by NDS employees Hasak, Norris, Adams, Gutman, and Segoli, among others, and implemented by NDS employees and/or agents Kommerling, Tarnovsky, and Menard, among others.

41. Defendant Oliver Kommerling a/k/a "Alex," "ALEX," "Alexander," "Oli," "Oli K," "Oliver Kiss," and "OK" ("Kommerling") is an individual and

citizen of Germany, residing in Monaco. During all times relevant as stated herein, Kommerling was either: (a) working for, at the direction of, and under the direct and/or indirect control of NDS, and with NDS's full knowledge and/or ratification, as well as for his own individual interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system; or (b) working in concert with NDS, its employees and/or agents in serving his role in the overriding NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system.

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

43. In 1999, Kommerling and Markus Kuhn co-wrote "Design Principles for Tamper Resistant Smartcards." This publication became one of the standard texts 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, among others.

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

Access Cards and assisted in physically extracting the Canal+'s SECA ROM code contained therein. Kommerling further declared that the code he assisted NDS in extracting was the same code that was published on www.dr7.com, the website owned, operated, and maintained by Menard. Specifically, Kommerling's declaration accuses NDS's double agent Tarnovsky of publishing the Canal+ SECA ROM code on the Internet.

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

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

47. Shortly thereafter, Mullen contacted Kommerling to discuss Kommerling's initial offer. During this second conversation, Kommerling stated that the "DISH Network fix" was being extracted at a sophisticated laboratory in Europe and that it was near completion. Kommerling also informed Mullen that Kommerling was involved in establishing this new state-of-the-art laboratory that

could hack anything related to DISH Network. In exchange for Mullen not releasing the full software fix for DirecTV's H-card, Kommerling represented that he was authorized to offer Mullen an exclusive deal to distribute the software for both DirecTV and DISH Network.

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

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

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

access system.

51. On March 13, 1998, at the direction of NDS and Kommerling, Luyando met with Mullen, Archie Timuik and Joseph Lucker in Windsor, Ontario to discuss Kommerling's authority to offer the "DISH Network fix," among other things. During this meeting Luyando represented to Mullen that Luyando was Kommerling's partner, that Luyando had Kommerling's full permission to negotiate with Mullen, and that Kommerling was authorized to sell Mullen the "DISH Network fix." During this meeting, at the direction of NDS and Kommerling, Luyando offered Mullen the full DISH Network "ROM dump" for "$1,000,000 USD." Luyando assured Mullen that he would be the *only* person with the fix and that he could "run with this for a long time." Luyando further represented to Mullen that the DISH Network ROM dump was acquired by Kommerling in a highly sophisticated laboratory. Concerning software, information, and technical support services, Luyando represented that Kommerling had access to "the most sophisticated equipment on the planet" and that the proceeds from the sale of the "DISH Network fix" were going to be "reinvested into more equipment that would help us all keep up with any new card swaps with DISH Network." Luyando informed Mullen that NDS, through Kommerling, instructed him to deal with Mullen first concerning a possible purchase of the "DISH Network fix," but that if Mullen was not interested, to approach others with the offer.

52. Defendant Plamen Donev a/k/a "Pluto," "Pman," "Digital," "Alien," "VIP," "Sadman," "Bolger," or "Bulgarian" ("Donev") is an individual and citizen of Bulgaria, residing in Sofia, Bulgaria. During all times relevant as stated herein, Donev was either: (a) working for, at the direction of, and under the direct and/or indirect control of NDS, and with NDS's full knowledge and/or ratification, as well as for his own individual interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a wide-spread

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

53. Defendant Vesselin Nedelchev a/k/a "Vesco," "VIP," "Bolger," "Vaseline," or "Bulgarian" ("Nedelchev") is an individual and citizen of Bulgaria, residing in Kazanlak, Bulgaria. During all times relevant as stated herein, Nedelchev was either: (a) working for, at the direction of, and under the direct and/or indirect control of NDS, and with NDS's full knowledge and/or ratification, as well as for his own individual interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system; or (b) working in concert with NDS, its employees and/or agents in serving his role in the overriding NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system.

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

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

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

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

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

58. Tarnovsky has been employed by NDS as a double agent from as early as 1997. Tarnovsky's role as NDS's double agent was to infiltrate hacking organizations and to report satellite piracy information back to NDS. However, upon going to work for NDS, Tarnovsky never stopped his hacking activities, which NDS is fully aware of, and is one of the main reasons he was hired by NDS. Upon NDS's instruction, including that by Norris, Hasak, Adams, and Gutman, Tarnovsky would obtain conditional access codes for NDS's competitors from NDS

and then Tarnovsky would make these codes available to Menard, owner and proprietor of the www.dr7.com website, for financial gain – and ultimately publication. Tarnovsky was paid by NDS for his double agent work, approximately $10,000 per month, in addition to being paid by hackers for his continued hacking activities, of which NDS was fully aware and openly acknowledge.

59. NDS, through Norris, Hasak, Adams, and Gutman, among others, were all kept well informed about the double agent role of Tarnovsky and sanctioned all of his hacking activities of EchoStar/NagraStar's Security System. On or about October 31, 1999, Tarnovsky posted on the DR7 pirate chat forum concerning EchoStar/NagraStar that "Echo is in bed with Nagra and will use same ROM for all their cards around the world." On December 24, 2000, using the nickname "nIpPeR cLaUz 00'," and under the direction and control of NDS, and with NDS's full knowledge and ratification, Tarnovsky posted a sequence of events and data, along with accompanying instructional code, that provided satellite pirates around the world the 'road map' and requisite instructions for the dump of Plaintiffs' entire EEPROM Code. Tarnovsky posted the foregoing, which was illegally obtained by NDS in its Haifa, Israel lab and sent to Tarnovsky via Hasak and Norris with the specific instructions to effectuate and assist others in effectuating a wide spread compromise of Plaintiffs' conditional access system, on the Internet website www.piratesden.com. In addition to allowing these satellite pirates to procure a dump of Plaintiffs' ROM and EEPROM Codes and accompanying secret keys, the December 23 and 24, 2000 postings and assistance provided by NDS, Tarnovsky and Menard, among others, also provided these same hackers with the necessary instructional codes and commands to gain unlawful access to the internal workings of the embedded microprocessor and 'read' and 'write' to same. With this assistance, satellite pirates around the world now had the all the requisite proprietary information once secured in Plaintiffs' microprocessor. Specifically, with this December 23 and 24, 2000, assistance by NDS, Tarnovsky and Menard,

among others, satellite 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, among others, for obtaining reprogrammed EchoStar Access Cards. Consequently, NDS's goal of effectuating and assisting others in effectuating a wide-spread compromise of Plaintiffs' security system began to rapidly materialize.

60. Upon information and belief, discovery will reveal that Tarnovsky continued to provide assistance and/or facilitation of the unlawful piracy of Plaintiffs' DISH Network signal up through and including June 25, 2003 – shortly after Plaintiffs' filed the instant action.

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

62. Menard is a close personal friend, and business partner, of Tarnovsky. Menard, using the fictitious name "Al" and "DR7" and doing business as "X-Factor Design, Inc.," "NCRYPT," "Hi-Fi Audio Exchange," and "Regency Audio" is the owner of the www.dr7.com pirate website which served as a meeting and discussion forum of satellite pirates worldwide. Menard's website also served as Menard's business, among others, and were operated and utilized as an *alter ego* of Menard, and others currently unknown to Plaintiffs, for the purpose of furthering

Defendants' scheme to defraud Plaintiffs. Menard unlawfully published the master keys and ROM and EEPROM Codes on www.dr7.com of the following satellite providers: DirecTV, Canal+, and DISH Network. Menard received these proprietary Codes from NDS through Tarnovsky acting on behalf of and under the control and direction of NDS. Menard's website continued to provide assistance and support to satellite pirates around the world in furtherance of NDS's objectives until approximately June 21, 2001, the date in which www.dr7.com was shut down.

63. Upon information and belief, discovery will reveal that Menard continued to provide assistance and/or facilitation for the unlawful piracy of Plaintiffs' DISH Network signal up through and including June 21, 2001, when he shut down his website www.dr7.com.

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

65. Wilson was the Registrant for the domain name of Menard's pirate website, "www.dr7.com." Wilson is also listed as the Billing Contact and Administrative Contact for Menard's company, X-Factor Web Design, Inc., at 11215 Jasper Ave. NW, Suite 435, Edmonton, Alberta Canada T5K OL5.

66. Upon information and belief, discovery will reveal that Wilson continued to provide assistance and/or facilitation for the unlawful piracy of Plaintiffs' DISH Network signal up through and including June 21, 2001, when the

website www.dr7.com was shut down.

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

68. Main, using the fictitious name of "Rymer," worked for Menard and his company, X-Factor Design. Main's job responsibilities included trafficking, conspiring to traffic, and/or assisting others in the trafficking of illegal drugs, Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices, and currencies related to illegal drugs and illegal signal theft devices. On or about August 30, 2001, concerning Tarnovsky's receipt of $40,100 from his mailbox address in San Marcos, Texas, a report from the Royal Canadian Mounted Police's Latent Fingerprints Operations positively identified the fingerprints lifted from the "Pioneer DVD" player and the "JVC DISC" to Main. These monies, among others, were payment from Menard to Tarnovsky (via Main) for Tarnovsky's assistance in designing, manufacturing, altering, and reprogramming EchoStar Access Cards or other Circumvention or Signal Theft Devices and providing software, information, and technical support services for the continued maintenance of illegal Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices.

69. Upon information and belief, discovery will reveal that Main continued to provide assistance and/or facilitation for the unlawful piracy of Plaintiffs' DISH Network signal up through and including June 21, 2001 when the

website www.dr7.com was shut down.

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

71. Dawson, using the fictitious names of "JD," "Jack Daniels," and "Dave" and doing business as "Discount Satellite," "DiscSat," and "DSScanada," was one of the pirate dealers working under Menard who was involved with selling Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices. Dawson received his Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices from Menard and, in turn, acted as a "dealer" and distributed and sold Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices for profit. Dawson also advertised the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the State of California and elsewhere through advertisements placed by Dawson in one or more "underground" satellite pirate publications, and through his Internet websites, www.discountsatellite.com and www.DSScanada.com, and email addresses created, operated, and maintained by Dawson. Upon information and belief, Discount Satellite, DiscSat, and DSScanada are or were owned, operated, and utilized as an *alter ego* of Dawson, and others currently unknown to Plaintiffs, for the purpose of furthering Defendants' scheme to defraud Plaintiffs. Dawson

engaged in the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the United States.

72. Dawson continued to engage in the illegal advertisement, sale, and distribution of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in furtherance of NDS's objectives until approximately May 20, 2000, the date in which www.discountsatellite.com was shut down, and until approximately June 19, 2003, the date in which www.dsscanada.com was shut down.

73. Defendant Shawn Quinn a/k/a "Hitec" d/b/a "HitecSatellite" and "HitecSat" ("Quinn") is an individual and citizen of Canada, residing in British Columbia. During all times relevant as stated herein, Quinn was either: (a) working for, at the direction of, and under the direct and/or indirect control of NDS, and with NDS's full knowledge and/or ratification, as well as for his own individual interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system; or (b) working in concert with NDS, its employees and/or agents in serving his role in the overriding NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system.

74. Quinn, using the fictitious name "Hitec" and doing business as "HitecSatellite" and "HitecSat," was one of the pirate dealers working under Menard who was selling Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices. Quinn received his Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices from Menard and, in turn, acted as a "dealer" and distributed and sold the Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices for profit. Quinn also advertised the sale of Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices in the State of California and elsewhere

through advertisements placed by Quinn in one or more "underground" satellite pirate publications, and through his Internet website, www.hitecsat.com, and email addresses created, operated, and maintained by Quinn. Upon information and belief, "HitecSatellite" and "HitecSat" are or have been operated and utilized as an *alter ego* of Quinn and others currently unknown to Plaintiffs for the purpose of furthering Defendants' scheme to defraud Plaintiffs. Quinn engaged in the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the United States.

75. Quinn continued to engage in the illegal advertisement, sale, and distribution of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in furtherance of NDS's objectives until approximately June 19, 2003, the date in which www.hitecsat.com was shut down.

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

77. Sergei, using the fictitious name "Koin" and doing business as "Koinvizion," was one of the pirate dealers working under Menard who was selling Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices. Sergei received his Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices from Menard and, in turn, acted as a "dealer" and distributed and sold the Pirated EchoStar Access Cards and/or other Circumvention or Signal

Theft Devices for profit. Sergei also advertised the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the State of California and elsewhere through advertisements placed by Sergei in one or more "underground" satellite pirate publications, and through his Internet website, www.koinvizion.com, and email addresses created, operated, and maintained by Sergei. Upon information and belief, Koinvizion was owned, operated, and utilized as an *alter ego* of Sergei and others currently unknown to Plaintiffs for the purpose of furthering Defendants' scheme to defraud Plaintiffs. Sergei engaged in the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the United States.

78. Sergei continued to engage in the illegal advertisement, sale, and distribution of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in furtherance of NDS's objectives until approximately January 28, 2001, the date in which www.koinvizion.com was shut down.

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

80. Frost, using the fictitious name "Frosty" and doing business as "The New Frontier Group," was one of the pirate dealers working under Menard who was selling Pirated EchoStar Access Cards and other Circumvention or Signal

Theft Devices. Frost received his Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices from Menard and, in turn, acted as a "dealer" and distributed and sold the Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices for profit. Frost also advertised the sale of Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices in the State of California and elsewhere through advertisements placed by Frost in one or more "underground" satellite pirate publications, and through his Internet website, www.newfrontiergroup.com, and email addresses created, operated, and maintained by Dawson. Upon information and belief, The New Frontier Group was owned, operated, and utilized as an *alter ego* of Frost, and others currently unknown to Plaintiffs, for the purpose of furthering Defendants' scheme to defraud Plaintiffs. Frost engaged in the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the United States.

81. Frost continued to engage in the illegal advertisement, sale, and distribution of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in furtherance of NDS's objectives until approximately June 25, 2003, the date in which www.newfrontiergroup.com was shut down.

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

83. Dale was one of the pirate dealers working under Menard who was

selling Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices. Dale received his Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices from Menard and, in turn, acted as a "dealer" and distributed and sold the Pirated EchoStar Access Cards and/or other Circumvention or Signal Theft Devices for profit. Dale engaged in the sale of Pirated EchoStar Access Cards and other Circumvention or Signal Theft Devices in the United States.

84. Defendant George Tarnovsky a/k/a "George Vladimar," "Vlad," and "Joe Zee" ("Tarnovsky Sr.") is an individual and citizen of the United States, residing in Virginia. During all times relevant as stated herein, Tarnovsky Sr. was either: (a) working for, at the direction of, and under the direct and/or indirect control of NDS, and with NDS's full knowledge and/or ratification, as well as for his own individual interest and/or gain, as a participant in the overriding NDS conspiracy to effectuate and/or facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system; or (b) working in concert with NDS, its employees and/or agents in serving his role in the overriding NDS conspiracy to effectuate and facilitate others in effectuating a wide-spread compromise of Plaintiffs' conditional access system.

85. Upon information and belief discovery will also reveal that Tarnovsky Sr., acting under the direction and control of NDS via Norris, took steps to actively conceal his son's involvement in the wrongdoing alleged herein. Specifically, Plaintiffs are informed and believe that after Norris learned that certain third parties had documentary proof that Tarnovsky was involved in the distribution network, Norris sent Tarnovsky Sr. – acting under the fictitious name "Joe Zee" – to remove and delete all such evidence in the possession of this third party.

86. Defendant Brian Sommerfield a/k/a "HeeD" ("Sommerfield") is an individual and citizen of Canada, residing in British Columbia. During all times relevant as stated herein, Sommerfield was either: (a) working for, at the direction

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

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

88. Defendant "Beavis" true identity unknown at this time.

89. Defendant "jazzercz" true identity unknown at this time.

90. Defendant "Stuntguy" true identity unknown at this time.

91. Upon information and belief discovery will reveal that Defendants NDS, NDS Americas, Norris, Hasak, Kommerling, Luyando, Donev, Nedeltchev, Tarnovsky, Menard, Main, Wilson, Dawson, Quinn, Sergei, Frost, Dale, Tarnovsky Sr., Sommerfield, Bruce, "Beavis", "Jazzercz" and "Stuntguy" 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 Plaintiffs' Access 'Smart' Cards; (b) software, hardware, Pirated

EchoStar Access Cards and/or other circumvention or 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.

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

IV. RELATIONSHIP BETWEEN NDS AND THE INDIVIDUAL DEFENDANTS

A. Direct Employment Relationship

The following individual Defendants are, and were at all times relevant as stated herein, directors, officers, and/or employees acting under the direction and control of NDS PLC and/or NDS, Americas: (1) Norris; (2) Hasak; (3) Tarnovsky; (4) Tarnovsky, Sr.; (5) Kommerling; (6) Luyando; (7) Donev; and (8) Nedeltchev.

B. Agency Relationship

(1) **Agency/Sub-Agency**: The following individual Defendants were, at all times relevant as stated herein, agents and/or sub-agents of NDS PLC

and/or NDS Americas acting at all times under the direct and/or indirect control of NDS (through Norris and/or Tarnovsky) and in furtherance of NDS's ultimate goals of effectuating and/or facilitating others in effectuating the wide-spread compromise of Plaintiffs' security and ultimately eliminating Plaintiffs as a competitor of NDS in the CAS marketplace:

(a) **Menard**: 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 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, Dale, and Frost. 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.

(b) **Dawson, Quinn, Sergei, Dale, and Frost**: As stated, NDS via Tarnovsky directed Menard to solicit the help of a select group of distributors for the unlawfully reprogrammed EchoStar Access Cards and other Circumvention or 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 Circumvention or Signal Theft Devices in a manner that NDS could control. Because Tarnovsky and Menard solicited the help of Dawson, Quinn, Sergei, Dale, and Frost to act on behalf of NDS and under NDS's control via Tarnovsky and Menard, Defendants Dawson, Sergei, Quinn, Dale, and Frost thereby became sub-agents of NDS. And, in accordance with serving out their role as distributor sub-agents in the overriding NDS conspiracy, Defendants Dawson, Quinn, Sergei, Dale, and Frost facilitated the compromise of Plaintiffs' Security System by trafficking in, among others, illegally reprogrammed EchoStar Access Cards and other Circumvention or Signal Theft Devices.

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

(d) **Bruce**: Menard's agent Quinn additionally solicited the assistance of Defendant Bruce to help in establishing and operating NDS's distribution network. Upon being approached by Quinn, Defendant Bruce agreed to assist in the NDS/Tarnovsky/Menard distribution network by, among other acts, hosting Quinn's hacker website www.hitecsat.com. And, because Quinn's solicitation of Defendant Bruce was a foreseeable result of NDS's agency relationship with Menard and subagency relationship with Quinn, in addition to the fact that Defendant Bruce acted in furtherance of NDS's ultimate goals and NDS

accepted the benefit of such acts, Defendant Bruce was not only an agent of Quinn, but also a sub-agent of NDS.

(2) **Agency by Ratification**: Defendants Menard, Dawson, Sergei, Quinn, Frost, Dale, Main, Wilson and Bruce also became NDS's agents by subsequent ratification. To be sure, NDS: (1) had actual or constructive notice of the unlawful acts engaged in by Menard, Dawson, Sergei, Quinn, Frost, Dale, Main, Wilson and Bruce in furtherance of carrying out NDS's objectives through the distribution network; and (2) accepted and/or retained the benefits and commercial advantage obtained through the acts of Defendants Menard, Dawson, Sergei, Quinn, Frost, Dale, Main, Wilson and Bruce. 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.

(3) **Agency by Estoppel**: Defendants Menard, Dawson, Sergei, Quinn, Frost, Dale, Main, Bruce and Wilson also became NDS's agents and/or sub-agents under the doctrine of estoppel. As with ratification outlined above, by NDS knowingly accepting the benefits and commercial advantage obtained through the acts and omissions of Defendants Menard, Dawson, Sergei, Quinn, Frost, Dale, Main, Bruce and Wilson, NDS is estopped from contesting its agency and/or sub-agency relationship with same.

C. Co-Conspirators of NDS and NDS, Americas

The following individual Defendants were at all times relevant herein acting as co-conspirators of NDS PLC and/or NDS Americas in serving their role in materializing 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) Tarnovsky Sr.; (5) Kommerling; (6) Donev; (7) Vesco; (8) Luyando; (9) Menard;

(10) Wilson; (11) Main; (12) Dawson; (13) Quinn; (14) Sergei; (15) Dale; and (16) Frost.

In addition to their employee or agency relationship with NDS, the foregoing Defendants were also acting in concert with NDS as co-conspirators vis-à-vis the overriding NDS conspiracy to eliminate Plaintiffs from the CAS marketplace. NDS conspired with and through their directors, officers, and/or employees (Norris, Hasak, Tarnovsky, Tarnovsky Sr., Kommerling, Luyando, Donev, and Vesco) to effectuate and facilitate others in effectuating the wide-spread 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, Dale, Main and Wilson to provide assistance in carrying out NDS's goals of assisting others in compromising Plaintiffs' Security System.

V. PLAINTIFFS' & DEFENDANT NDS'S SECURITY SYSTEMS

A. The Components of Plaintiffs' Security System.

93. 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").

94. 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)

95. 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, among other things, a microprocessor unit. The microprocessor unit performs and stores data and encryption technology and performs various computing and customer entitlement functions enabling, among other things, 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,

96. The microprocessor unit is supported, in part, 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.

97. 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.

98. 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.

99. 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.

100. At the first activation of a customer's set-top box, EchoStar sends a signal to the Access Card in order to "pair" the Access Card to the set-top box. Both the Access Card and set-top box have a unique identification number that is maintained by EchoStar's subscriber management system. This pairing operation, utilizing the two unique identification numbers, is mandatory for the proper operation of Plaintiffs' Security System.

101. 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: (a) certain aspects of the software and/or codes used in Plaintiffs' CAS; (b)

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

102. 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.

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

104. 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.

105. 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. Upon information and belief, NDS was able to dictate when its Access Cards would be hacked, and thus, could continue to make money from its customers, such as DirecTV, for Access Card swap-outs and for providing ECMs to the NDS hackers' latest piracy efforts.

106. Upon information and belief discovery will demonstrate that NDS made the conscious decision to manipulate the hacking of its own Security System

and to get the most possible financial gain from the hack of its Access Card. With most of the world's best pirates on its payroll, 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.

107. 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. During this swap out period, DirecTV used both the "P1" and "P2" conditional access systems. On or about July 7, 1997, the swap out was complete and the "P1" system was shut down completely.

108. Unfortunately for DirecTV, because NDS had put all of the world's best hackers on its payroll, NDS was fully aware of, and sanctioned, the hack of its P2 cards, notwithstanding the swap out agreed to by DirecTV. By the end of August 1997 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.

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

110. 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.

111. 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.

112. 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.

113. 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' CONSPIRACY, COMMON PLAN & UNLAWFUL CONDUCT

A. PHASE 1: (The Formation of an Employer/Employee and/or Principal/Agent relationship Between NDS and Many of the Named Defendants) 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.

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

MAIN STORY

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

We must face the fact that our [NDS's] reputation is bad and our competitors make capital out of it. We can claim that P11 is not hacked but how confident we be of the technology. Part of the reason 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.

In listening to Alex [Oliver Kommerling], who is not allowed to hack P11 [NDS smartcard], and coupling that with what is said by others I 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.

. . . The techies must realize that their technology has not been put to the test because largely we are stopping it [by controlling the 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.

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

The result of more hacks will be a loss of confidence and a loss of business. At present we are not gaining most of the new projects. How long before we actually lose one to a competitor.[12] *Our jobs are on the line. Maybe not yet but we are vulnerable.*

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

[12] 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.

forums, states:

> *Chris Tarnovsky*
> *When Scheel was in Canada he wrote to Biggun[Tarnovsky] (using Anthony's computer and email account) asking for help. At that time Biggun wrote back saying that the man behind Marty Mullin's hack is named Dieter. It was only after he returned to Germany that Oliver [Kommerling] told him that Chris Tarnovsky is Biggun.*
>
> *Anthony has told Scheel that Chris Tarnovsky has gone underground because he had made promises to the group he was working for and could not deliver.*

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

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

116. On or about October 21, 1997, an NDS Memorandum, concerning Tarnovsky using the nickname "Coleman" and NDS's control over Tarnovsky as one if its hacker/agents, states:

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

117. On or about October 22 – 24, 1997, an NDS Memorandum, establishes that John Luyando [nicknamed "Yanni" and "Jellyfish"] was working for NDS as a hacker/agent as early as October 1997 and that NDS concealed to DirecTV that Kommerling was also a hacker/agent employed by NDS. An "urgent" NDS memorandum concerning Kommerling and Luyando was written to Adams

indicating that Larry Rissler, Vice President of Signal Integrity for DirecTV, had contacted NDS and was inquiring as to whether Kommerling was working for NDS. Rissler asked Norris about an individual named "Oli K" or "Oliver Kiss." Rather than being forthright with DirecTV – NDS's largest client that NDS was fighting desperately to retain notwithstanding DirecTV's utter disappointment with NDS's consistently compromised Security System – Norris lied to Rissler in an attempt to conceal Kommerling's relationship with NDS.

118. In an effort to continue to conceal NDS's relationship with Kommerling, the memo advises Adams that "*Oliver [Kommerling] should not travel with luyando in the future. I prefer all contact (call [sic], email, etc) be discontinued at this point but this can not [sic] happen due to Oliver's [Kommerling] standing in the hacker community.*" A follow up facsimile from Adams to Hasak concerning the possibility that DirecTV was setting a trap for NDS hackers Kommerling and Luyando to be arrested when attempting to get onto an airplane, and NDS's actions to circumvent any incrimination of Kommerling, states:

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

119. On or about November 10, 1997, NDS Letter from Norris to Adams concerning the "batulator" and Tarnovsky's hacking ability states: "*fyi, the*

'compulator' aka 'batulator' code was reversed by Mike [Tarnovsky] several weeks ago and the heart has been exposed...." At this time, Tarnovsky was an employee and agent of NDS and was acting on behalf of and at the direction of NDS.

120. 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."[13]

121. 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 atmosphere was very open and, in my opinion, was a good discussion. The discussion was around Boris [Floricic][14] 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*

[13] 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 officials that: (a) the equipment in Tarnovsky's home – which included various pirating devices such as a card emulator – was property of NDS; (b) Tarnovsky had been an NDS employee since February 1, 2001; and (c) the U.S. Customs' officials were not to search Tarnovsky's home without a search warrant.

[14] 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."

> *its product. (Yossi said: 'There's a limit to how far out I will stretch my neck out for Rupert Murdoch')*[15]

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

> Yossi and Alex [Kommerling] also raised a possible scenario, which, to the best of my knowledge, has not been considered. *Alex [Kommerling] pointed out that it is very easy to trace the transport of Fed-Ex packages or other postal packages.* It would be no problem for a journalist to find that *there have been very frequent exchange [sic] of postal packages between Alex [Kommerling] and NDS-UK and NDS-Israel. What would happen if a journalist came knocking on Alex's [Kommerling's] door with a Camera? . . . Yossi said he would like a contingency plan developed for such a scenario.*

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

123. On or about June 18, 1999, an NDS Letter to Hasak from Adams concerning NDS's hiring satellite pirates and hackers in order to "CONTROL" them, as well as NDS's fear of losing its contract with DirecTV to be DirecTV's smart card provider, 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*

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

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.[16]

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 Smart Card Swaps

124. 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 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.

125. On or about December 1, 1997, an NDS Memorandum entitled "Operations Security Group" from Gutman to Hasak, Segoli, Adams, and Norris regarding a "Global View - 12/1/97," concerning NDS's placement of Tarnovsky

[16] 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.

into Ron Ereiser's pirate organization with NDS's full support, states: "*Ron Ereiser's Group - hired Tarnovsky to Calgary . . . CT [Tarnovsky] was tasked with creating four secure programmer boxes [illegal NDS Smart Card programmers]. Each member of the group will receive a box, thus enabling the programming of more cards and ensuring that if one of them gets caught - the business of selling 3Ms [DirecTV hack] will continue.*" Concerning NDS's technical support for his 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.

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

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

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

128. On or about December 1998, a Letter is sent from Adams to Hasak regarding "Week Report," and concerning Alex [Kommerling] Adams references NDS's secret Black Hat Team, " . . . *you and I believed that Alex [Kommerling]*

was moving into a managerial role and would be a leader of black hat activity [illegal hacking and pirating of competitor's access cards]." Further, concerning Kommerling's role with NDS, and the reason NDS and Kommerling formed the company ADSR, and NDS's hacking of the Galaxy Smart Card, Adams writes:

> *. . . he absolutely misinterpreted the whole reason we have formed ADSR [a company owned 60% by Kommerling and 40% by NDS]. 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].*
>
> . . . .
>
> *It should be a simple task for one of our techies to prove that the Australian Irdeto card is as vulnerable [hack the card] as any in any other country.*
>
> *I can send Prince [an NDS agent] to Australia and he will visit Pirate dealers and get cards direct from them. Even Alex [Oliver Kommerling] and I could go and do it, want to come. I know that Galaxy has been pirated in the past. . . . What we need urgently are some official cards from each of the system, 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.*

129. On or about April 30, 1999, an NDS Letter from Adams to Hasak references a meeting that Kommerling had with Canal+, wherein Kommerling was asked about the www.DR7.com [Menard] Hack release. Kommerling was asked if he could do a hack of the "IRDeto" system in Arabia on PANAM SAT channel ART 1, however, unbeknownst to Canal+, the hack of IRDeto was already in NDS's possession. "*JR wants Alex [Kommerling] to hack the system but at the same time to provide a 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. You will recall the occasion when I was asked to get software urgently some 3 months ago. I did it and had to pay 10 [10,000 pounds]. Well that software only needs updating with the new keys. :-)*"

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 and other Defendants, NDS Built a Sophisticated Laboratory in Haifa, Israel, Where NDS Cracked Plaintiffs' Access Card and Obtained Their Secret ROM and EEPROM Codes.

130. The reason it takes sophisticated technology to perform an invasive attack on Access Cards is that, in order to develop a way to defeat a Security System, an individual or entity must know and understand how the system works. As a result, an individual or entity must have access to the software contained in the ROM and EEPROM contained in Access Cards. The software contained in ROM and EEPROM is written in machine language which is almost impossible for humans to use or understand because it consists entirely of binary digits. The foundry manufacturing the basic component of Access Cards uses advanced security designs and manufacturing techniques to render them tamper proof.

131. A hacker wanting to obtain the ROM and EEPROM software contained in EchoStar Access Cards would have to use a sophisticated laboratory equipped with a scanning electron microscope and/or focused ion beam, among other things. They would then have to analyze the chip mapping out the 1s and 0s and then reverse-compiling those numbers to have access to and understand the imbedded software. This also requires the involvement of very sophisticated and highly skilled programmers and engineers.

132. Kommerling testified in the *Canal+ v. NDS* case that NDS engineers at NDS's Haifa, Israel laboratory 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.

133. Plaintiffs are informed and believe that NDS engineers 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 set-top box that, in the ordinary course of its operation, authenticates which DISH Network Programming services legitimate subscribers are entitled to view.

134. Plaintiffs are informed and believe that NDS and its employees and agents hacked Plaintiffs' Security System, made an unauthorized and impermissible copy of the proprietary information and Codes contained in EchoStar Access Cards at the Haifa, Israel laboratory, and then transmitted Plaintiffs' proprietary information and Codes to NDS employee Tarnovsky who was residing in the United States [in the State of California]. One of Tarnovsky's tasks was to distribute this information in a manner designed to proliferate Pirated Access Cards and other Circumvention or Signal Theft Devices which could provide unauthorized users with access to EchoStar's DISH Network satellite television Programming services.

135. Based upon information and belief, NDS, at its laboratory in Haifa, Israel, (1) intentionally accessed the microprocessor of the EchoStar Access Cards without authorization, (2) physically extracted Plaintiffs' secret ROM and EEPROM Codes contained therein without authorization, (3) distributed Plaintiffs' secret ROM and EEPROM Codes to Tarnovsky with specific instructions for its dissemination, and (4) controlled the design, manufacture, and sale of 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 without authorization. NDS orchestrated this plan with the intent to defraud EchoStar of revenue from DISH Network subscriptions and to injure the effectiveness of Plaintiffs' Security System. NDS's improper motivation for engaging in this illegal anti-competitive conduct consisted of, among other reasons, a last ditch effort to retain the business of DirecTV, one of Defendants' largest accounts, who was on the verge of entering into contractual relations with NagraVision in an effort to obtain a more secure CAS to protect its satellite signal from unauthorized reception and decryption.

136. On or about November 29, 1999, a NDS Memorandum from "Mike" [Tarnovsky] reporting to NDS on the meeting Tarnovsky set up with Hannibal [Saggiori]. When asked who he worked for, "[Tarnovsky] *responded about working for 'Flagship Automation from Nashua, NH' as their fielded tech-support lead for WonderWare, Inc. I explained how we called the tool, 'UnderWare' instead and that it is a Windows hosted scripting language/gui program . . .*" when, in fact, Tarnovsky was actually working for NDS and had been since approximately 1997.

137. Concerning the EchoStar hack, Tarnovsky's Memorandum states: "*Hannibal [Saggiori] believes Alex [Kommerling] is working with the Canadians on the E* hack. I explained to him that the Canadians who are behind the hack. I told him Discount [Dawson] and Kerrobert Satellite [Ereiser] hated Alex [Kommerling] because he did not return nor help them with the 3 VideoCipher II Plus. I told him that due to this condition, it is unlikely Alex [Kommerling] is behind the E* break. I tried to make him rethink his assumptions on Alex [Kommerling] by use of the Canadians which does seem to have worked, however Hannibal [Saggiori] still believes the IRDeto and SECA [Canal+'s Code] are Alex's [Kommerling's and NDS's] doing.*"

138. On or about May 5, 2000, an NDS Memorandum concerning Tarnovsky and the EchoStar hack, states in relevant part: "*You will note that suspicion has fallen on MIKE [Tarnovsky]. This is because, as Hannibal*

[Saggiori] says, MIKE [Tarnovsky] was the person who introduced the Bolgers [Plamen Donev and Vesselin Nedeltchev] to the American/Canadian Pirates. Yet Hannibal [Saggiori] is the one named [in a lawsuit by DTV/NDS]. Thus Hannibal [Saggiori] concludes that MIKE [Tarnovsky] works for NDS. There are a series of threatening statements inasmuch that MIKE [Tarnovsky] is behind DR7 [Menard and www.dr7.com] and MIKE [Tarnovsky] hacked ECHOSTAR . . .."

2. Step 2: NDS Had to Provide the Illegally Obtained ROM and EEPROM Codes to a Software 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.

139. On or about November 19, 1995, Tarnovsky sent an e-mail to a "TV-Crypt" concerning his desire to begin hacking Access Cards, where he admits his status as a pirate and hacker: "*[m]y name is Chris Tarnovsky! I am a hacker/programmer very much into Electronics/Ham Radio/Modems/Video Access Control (!) and anything else out there I find interesting....I am a fanatic when it comes to Sky . . . Eagerly awaiting tearing into the code for the card!*"

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

141. On or about July 11, 1996, Tarnovsky sent an email to Jan Saggiori concerning Tarnovsky's and Saggiori's combined efforts to hack Access Cards. Concerning Tarnovsky's employment at "ULVAC" at the time, and the equipment at his disposal to hack Access Cards, Tarnovsky states: "*We [ULVAC] also have an*

E-beam tester downstairs . . . everything will be fine here once I am settled in place! For now, nothing for that [hacking] is possible. I am waiting for things to become "more comfortable" (!) ... Now, we need to find the SA for the CTV stuff and the old CANAL+/CINECINEMAS keys [secret keys to EEPROM or ROM] . . . *we want everything! . . . – Chris*"

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

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

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

145. On or about December 7, 1999, a post to the Internet by "Shrimp" [Tarnovsky] concerning Tarnovsky's knowledge of reverse engineering Access Cards and the cost of doing so, he states "*any chip can be reverse engineered to the point of understanding for under $110,000. The problem is they might be more devices which would need to be reversed and then the costs mount up.*" A post later this date by "GS2" affirms the relationship between Tarnovsky and Menard and states that "*Shrimp [Tarnovsky] is a very good friend of DR7 [Menard].*"

146. As illustrated by the proceeding factual allegations, 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, 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 23 and 24, 2000 disseminate Plaintiffs' proprietary information and Codes over the Internet.

b. NDS Approached Other Well-Known Hackers in its Decision to Compromise Plaintiffs' Security System and Disseminate Plaintiffs' Proprietary Codes.

147. Plaintiffs are informed and believe that, prior to obtaining the help of Tarnovsky, Menard, Dawson, Koin, Frost, Sergei, and Quinn, among others, NDS considered other methods of disseminating Plaintiffs' Codes and unlawful software support information necessary to accomplish the wide-spread compromise of Plaintiffs' CAS. Specifically, in sworn affidavit testimony obtained from Martin Paul Stewart (f/k/a Martin "Marty" Mullen), Mullen testifies as follows:

> In August 1997, I was contacted via telephone by an individual named Oliver Kommerling ("Kommerling"). *During this conversation, Kommerling introduced himself to me and informed me that he would soon be in possession of the first hack of the EchoStar/NagraStar ROM Code. Kommerling stated to me that this ROM Code was currently being extracted in a "highly sophisticated laboratory in Europe." Kommerling then informed me that he was able to offer me the hack on the EchoStar/NagraStar microprocessor and that he*

wanted to come to Canada and arrange a meeting to discuss the details. Kommerling said that he was informed that I was in possession of pirating software for the DirecTV H-Card and that if I delayed in releasing that software he was authorized to provide me with the DISH Network ROM Code. It is my understanding, after speaking with numerous individuals including, without limitation, Kommerling's agent John Luyando ("Luyando" or "Yanni"), as well 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).

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

Mullen Affidavit ¶ 21 (emphasis added).

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

Mullen Affidavit ¶ 22 (emphasis added).

> *During this meeting, "Yanni" informed us that Kommerling was authorized to offer us the DISH Network ROM Code for $1,000,000 USD*. During this March 13, 1998 meeting, "Yanni" informed us that Kommerling was willing to either set up a demonstration of the DISH 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 website and Chris Tarnovsky's postings on same, that this DISH Network ROM dump had been provided to another group known as the "Swiss Cheese" Group*.

Mullen Affidavit ¶ 26 (emphasis added)

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.

148. 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.

149. Menard was the only person to possess such a device for approximately a year and a half, or from 1999 until early 2001,[17] and thus, with the

[17] As a result of Tarnovsky's December 23 and 24, 2000 postings, satellite pirates and software