

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

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

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

Attorneys for Plaintiffs
EHOSTAR SATELLITE CORP., et al.

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

EHOSTAR SATELLITE
CORP., et al.,

Plaintiffs/
Counterclaim
Defendants,

v.

NDS GROUP PLC, et al.,

Defendants/
Counterclaim
Plaintiffs.

No. SA CV 03-950 DOC(JTLx)

**EHOSTAR'S FIFTH AMENDED
COMPLAINT (5AC) FOR:**

- 1) **Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1)(A);**
- 2) **Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2);**
- 3) **Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a);**
- 4) **Violation of RICO Statute, 18 U.S.C. § 1962(c);**
- 5) **Unfair Competition in Violation of California Business & Professions Code § 17200;**
- 6) **Violation of California Penal Code § 593d(a);**
- 7) **Violation of California Penal Code § 593e(b);**

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

JURY TRIAL DEMANDED

TABLE OF CONTENTS

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

| | | |
|------|--|----|
| I. | INTRODUCTION & NATURE OF THE CASE..... | 1 |
| II. | JURISDICTION & VENUE | 10 |
| III. | PARTIES & RELATIONSHIP TO PLAINTIFFS’ SUIT | 11 |
| IV. | RELATIONSHIP BETWEEN DEFENDANTS AND THEIR EMPLOYEES, AGENTS, SUB-AGENTS AND CO-CONSPIRATORS | 13 |
| A. | Direct Employment Relationship..... | 14 |
| B. | Agency Relationships..... | 14 |
| 1. | Agency/Sub-Agency..... | 14 |
| a. | Menard | 14 |
| b. | Dawson, Quinn, Sergei, and Frost..... | 15 |
| c. | Mervin Main | 16 |
| C. | Agency by Ratification | 16 |
| D. | Co-Conspirators of NDS Group and NDS Americas | 17 |
| V. | PLAINTIFFS’ & DEFENDANT NDS’S SECURITY SYSTEMS..... | 18 |
| A. | The Components of Plaintiffs’ Security System..... | 18 |
| B. | NDS was Fully Compromised as Early as 1995 and Was Losing Credibility in the Conditional Access System Market Place | 20 |
| C. | At DirecTV’s Request, in 1998 the Kudelski Group Competed With NDS for a Bid to Replace NDS’s Security System With Nagravision as the Security System to be Used by DirecTV.... | 21 |
| VI. | DEFENDANTS’ CONCERTED OR OTHERWISE INTERRELATED UNLAWFUL CONDUCT | 22 |
| A. | <u>PHASE 1</u> : NDS Hires the World’s most Infamous Hackers in order to “Control” the Hacking of its Access Cards and Security System -- in Lieu of Improving its Technology | 22 |
| 1. | With the World’s Most Infamous Hackers on its Payroll, NDS was able to Dictate When its Access Cards Would be Hacked, and Thus Could Make Additional Monies from its Customers by Selling ECMs and Ultimately Doing Expensive Card Swaps | 26 |

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

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

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

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

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

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

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

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

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

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

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

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

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

A. NDS Group..... 43

1 B. NDS Americas..... 44

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

3 D. Mervin Main..... 48

4

5 X. CAUSES OF ACTION 48

6 First Cause of Action:

7 (Circumventing Technological Measures Concerning Protected

8 and Copyrighted Works in Violation of the Digital Millennium

9 Copyright Act, 17 U.S.C. § 1201(a)(1)(A)) 48

10 Second Cause of Action:

11 (Manufacture of and Traffic in Signal Theft Technology and

12 Devices in Violation of the Digital Millennium Copyright Act,

13 17 U.S.C. § 1201(a)(2) 50

14 Third Cause of Action:

15 (Facilitating the Unauthorized Reception of Satellite Signals in

16 Violation of the Communications Act of 1934, as amended,

17 47 U.S.C. § 605(a))..... 52

18 Fourth Cause of Action:

19 (RICO, 18 U.S.C. § 1962(c))..... 54

20 Fifth Cause of Action:

21 (Unfair Competition, California Business & Professions Code

22 § 17200) 71

23 Sixth Cause of Action:

24 (Violation of California Penal Code § 593d(a)) 73

25 Seventh Cause of Action:

26 (Violation of California Penal Code § 593e(b)) 74

27 PRAYER FOR RELIEF 76

28 DEMAND FOR JURY TRIAL..... 81

1 EchoStar Satellite L.L.C., EchoStar Communications Corporation, EchoStar
2 Technologies Corporation and NagraStar LLC (“EchoStar” or “Plaintiffs”) hereby
3 file their Fifth Amended Complaint (“5AC”) against Defendants NDS Group PLC
4 and NDS Americas, Inc. (“NDS” or “Defendants”) and, in support thereof,
5 respectfully state the following:
6

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5 12. Step 1 required NDS to obtain the Read Only Memory (“ROM”) and
6 Electronically Erasable Programmable Read Only Memory (“EEPROM”) codes
7 (“Codes”) used in their competitors’ Access Cards. These proprietary codes form
8 the heart and soul of CAS providers’ security system and, as such, are secured and
9 embedded in the tiny microprocessor unit stored in the Access Card. To extract
10 these Codes, NDS needed a state-of-the-art laboratory, extremely sophisticated
11 equipment including a scanning electron microscope and focused ion beam, and
12 highly skilled engineers. There are only approximately six (6) of these labs in the
13 world – NDS owns one of them in Haifa, Israel, which was designed and built by
14 NDS with the assistance of Kommerling¹ and used by NDS to extract the ROM and
15 EEPROM Codes and keys utilized by NDS’s competitors.

16 13. Using its Haifa laboratory, NDS unlawfully and impermissibly cracked
17 Plaintiffs’ Access Card and extracted Plaintiffs’ secret proprietary ROM and
18 EEPROM Codes secured therein. NDS then used that information to develop a
19 hack methodology to attack and defeat EchoStar’s CAS. This was not the first time
20 NDS engaged in this unlawful conduct. On April 9, 2002, NDS employee/agent
21 Kommerling provided sworn testimony in another suit² brought by Canal+ against
22 NDS for anticompetitive conduct similar to the acts alleged herein. In his

23
24 ¹ In 1999, Kommerling and Markus Kuhn co-wrote “Design Principles for Tamper
25 Resistant Smart Cards.” This publication became the standard text on how to
26 “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.

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

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

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

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

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

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

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

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

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

25 ⁴ Eventually, the method of payments from Menard to NDS and Tarnovsky was
26 discovered by U.S. Customs officials who launched an investigation into
27 Tarnovsky’s activities of satellite piracy and money laundering. Notably, when this
28 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

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

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

20 20. As evidenced by a significant number of internet posts cited herein, the
21 end user pirates obtaining reprogrammed EchoStar Access Cards from NDS, via
22 Tarnovsky and Menard, became discontent with the inability of these pirated
23 Access Cards to withstand Plaintiffs’ ECMs. Specifically, with the
24 “CONTROLLED” distribution network designed and implemented by, among
25 others, NDS, Tarnovsky, and Menard, end users who purchased one of these
26 reprogrammed EchoStar Access Cards had to send them back to
27 Menard/Tarnovsky, either directly or through dealers Dawson, Quinn, Sergei, and
28 Tarnovsky’s home without NDS’s counsel being present.

1 Frost for “fixes” or “updates” each time Plaintiffs launched an ECM to disable the
2 pirated Access Cards.

3 21. **In December 2000**, NDS, Tarnovsky and Menard, effectuated and
4 assisted others in effectuating a wide-spread compromise of Plaintiffs’ conditional
5 access system. On these dates, using the nicknames such as “nIpPeR⁵ cLaUz 00”
6 and “NiPpEr2000” under the direction and control of NDS, and with NDS’s full
7 knowledge and ratification, Tarnovsky posted for the first time a sequence of
8 commands and data, along with accompanying instructional code, that provided
9 satellite pirates around the world the “road map” and requisite instructions for: (a)
10 the full dump of Plaintiffs’ secret ROM Code; (b) the full dump of Plaintiffs’
11 EEPROM Code and accompanying secret keys; and (c) the instructions on how to
12 internally “hack” or access the microprocessor contained in EchoStar Access Cards
13 thereby providing hackers the “exploit key” necessary to gain access to Plaintiffs’
14 microprocessor and subsequently read and write to Plaintiffs’ Access Cards.

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

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

24 _____
25 ⁵ The name “NiPpEr” used by Tarnovsky to post Plaintiffs’ proprietary information
26 is significant. Specifically, when Plaintiffs’ Security System was developed,
27 NagraStar’s engineers concealed the term “NiPpEr” in the very heart of the secret
28 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.

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

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

19 25. This unlawful conduct continued up to and including the following
20 dates on which the respective pirating websites were shut down: (1) Menard –
21 www.dr7.com – June 21, 2001; (2) Dawson – www.discountsatellite.com;
22 www.dsscanada.com – June 19, 2003; (3) Quinn – www.hitecsat.com – June 19,
23 2003; (4) Sergei – www.koinvizion.com – January 28, 2001; and (5) Frost –
24 www.newfrontiergroup.com – June 25, 2003.

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

1 federal officials arrived unannounced at his California home.

2 27. As a result of the conduct alleged herein, particularly the December
3 2000 postings by Tarnovsky with the assistance and direction of NDS, the
4 continued reprogramming of EchoStar Access Cards by Tarnovsky up to and
5 including January 9, 2001, and the unlawful operation of the distribution websites
6 by Menard, Dawson, Quinn, Sergei, and Frost up to and including June 25, 2003,
7 Plaintiffs have suffered and will continue to suffer substantial damages. Moreover,
8 *the December 2000 postings by NDS/Tarnovsky put at risk over 7.6 million of*
9 *Plaintiffs' Access Cards already distributed in the marketplace. Consequently, Step*
10 *4 of the NDS conspiracy rendered a global card-swap by Plaintiffs unavoidable.*

11 **II. JURISDICTION & VENUE**

12 28. Jurisdiction and venue are proper in this court. This Court has original
13 federal question subject matter jurisdiction over this action under 28 U.S.C. §§
14 1331 and 1338, the Communications Act of 1934, as amended, 47 U.S.C. §
15 605(e)(3)(A), the Digital Millennium Copyright Act, 17 U.S.C. § 1203, the
16 Racketeer Influenced and Corrupt Organizations Act ("RICO"), and 18 U.S.C. §
17 1965(b). Alternatively, this Court has subject matter jurisdiction of this action
18 under 28 U.S.C. § 1332(a)(1) by virtue of the complete diversity of citizenship of
19 the parties in an action in which the matter in controversy exceeds the sum or value
20 of \$75,000, exclusive of interest and costs. This Court also has supplemental
21 jurisdiction, pursuant to 28 U.S.C. 1367(a), over the California state law claims
22 asserted herein.

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

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

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

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

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

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

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

1 principal place of business at 90 Inverness Circle East, Englewood, Colorado
2 80112.

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

15 35. Defendant NDS Americas, Inc. (“NDS Americas”) is a Delaware
16 Corporation with its principal place of business in Newport Beach, California, and
17 its registered agent for service of process is John Workman, 3501 Jamboree Road,
18 Suite 200, Newport Beach, California. As alleged herein, NDS Americas assisted
19 Tarnovsky in: (a) using the ROM and EEPROM codes extracted from Plaintiffs’
20 microprocessor by NDS Group to design and build a reprogramming device and
21 using same to modify EchoStar Access Cards up to and including January 9, 2001;
22 (b) creating and maintaining a controlled distribution network through which
23 reprogrammed EchoStar Access Cards could be sold, up to and including June 25,
24 2003; (c) providing technical support for these reprogrammed cards thereafter up to
25 and including June 25, 2003; and (d) posting the instructional code necessary for
26 others to hack Plaintiffs’ microprocessor on the world wide web in December 2000.

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

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

16
17 **IV. RELATIONSHIP BETWEEN DEFENDANTS AND THEIR**
18 **EMPLOYEES, AGENTS, SUB-AGENTS AND CO-CONSPIRATORS**

19 37. To clarify, Plaintiffs are not predicated the entire 5AC on any alleged
20 "unified course of fraudulent conduct." Rather, Plaintiffs' claims are based on a
21 multi-layered conspiratorial web consisting of corporate entities seeking to gain
22 dominance in the CAS marketplace and individuals seeking to profit from serving
23 their respective roles in carrying out this anticompetitive objective. Consequently,
24 Plaintiffs' claims are based on a course of anticompetitive conduct and *not* any
25 alleged course of "unified fraudulent conduct". As seen *infra* in the Causes of
26 Action section, Plaintiffs are asserting both direct and indirect theories of liability
27 against Defendants. In support of those respective theories, Plaintiffs have included
28

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

3 **A. Direct Employment Relationship**

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

15 **B. Agency Relationships**

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

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

25 **a. Allen Menard**

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

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

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

22 **b. Dawson, Quinn, Sergei, and Frost:**

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

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

4 43. In accordance with serving out their roles as distributor sub-agents in
5 the implementing NDS's objectives, Dawson, Quinn, Sergei, and Frost facilitated
6 the compromise of Plaintiffs' Security System by advertising, selling, distributing,
7 providing, and/or otherwise trafficking in, among others, illegally reprogrammed
8 EchoStar Access Cards and/or other Signal Theft Devices. The medium used for
9 this unlawful conduct was the internet through several pirating websites. The
10 NDS/Tarnovsky/Menard distribution network continued to operate and engage in
11 the acts underlying Plaintiffs' claims up to and including: (1) Menard –
12 www.dr7.com – June 21, 2001; (2) Dawson –www.discountsatellite.com;
13 www.dsscanada.com – June 19, 2003; (3) Quinn – www.hitecsat.com – June 19,
14 2003; (4) Sergei – www.koinvizion.com – January 28, 2001; and (5) Frost –
15 www.newfrontiergroup.com – June 25, 2003.

16 c. **Mervin Main:**

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

25 C. **Agency by Ratification:**

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

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

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

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

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

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

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

9 **V. PLAINTIFFS' & DEFENDANTS' SECURITY SYSTEMS**

10 **A. The Components of Plaintiffs' Security System.**

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

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

22 The Smart Card remains the property of EchoStar . . . and
23 *any tampering or unauthorized modification to the*
24 *Smart Card is strictly prohibited and may result in, and*
25 *subject you to, legal action.* You agree to return the
26 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).

27 51. EchoStar Access Cards are essential to the operation of the DISH
28

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

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

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

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

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

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

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

15
16 **B. NDS Was Fully Compromised as Early as 1995 and Was Losing**
17 **Credibility in the Conditional Access System Market Place.**

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

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

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

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

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

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

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

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

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

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

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

10 **VI. DEFENDANTS' CONCERTED OR OTHERWISE INTERRELATED**
11 **UNLAWFUL CONDUCT**⁶

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

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

19 68. By at least October 6, 1997, NDS was employing both Tarnovsky and
20 Kommerling in an effort to control the compromise of NDS's encryption
21 technology. On or about this same date, NDS, Hasak and Norris received an
22 internal memorandum from NDS employee Segoly discussing Tarnovsky and the
23 control NDS retained over Tarnovsky's interaction with other satellite pirates. In
24 this same memorandum, Segoly (a) acknowledges the high level of hacking
25

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

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

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

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

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

21 72. On or about November 13, 1997, is the first reference that Larry
22 Rissler, Vice President of Signal Integrity for DirecTV, could locate in his notes to
23 "Mike," one of the names used by John Norris to refer to Tarnovsky. It is Mr.
24 Rissler's recollection that Norris previously told him that he [Norris] had recruited
25 Tarnovsky to work as a consultant for NDS, and that Norris had moved Tarnovsky
26 to California."⁷

27 ⁷ In contrast, Norris was not so forthright with U.S. Customs agents when
28 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

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

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

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

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

22 76. On or about June 18, 1999, Hasak received an internal letter from
23 officials that: (a) the equipment in Tarnovsky’s home – which included various
24 pirating devices such as a card emulator for use in reprogramming EchoStar Access
25 Cards, among other unlawful purposes – was property of NDS; (b) Tarnovsky was
26 an NDS employee for years; and (c) the U.S. Customs officials were not to search
27 Tarnovsky’s home without a search warrant.

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

⁹ Rupert Murdoch’s News Corp. is the parent company of NDS.

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

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

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

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

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

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

19 *The one hostage that we carry into all these deliberations is the*
20 *weaknesses in our [NDS's] technology [Access Cards]. I have*
21 *not told you before as i assume you already know the same as*
22 *me. Yossi admits that our cards are even more vulnerable to*
23 *attack than anyone realised before. Glitching is practically a*
24 *magic key to access our cards. . . .*

25 *So given that the technology can be hacked very quickly what*
26 *do we do. Do we abandon recruitment [of other satellite*
27 *pirates and hackers] and leave everything to ECM's [electronic*
28 *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.

1
2 . . . *What we need is support. In the main that is money, money, money.*

3
4 *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.*

5
6
7 *... JOD was heavily involved in the DTV negotiations. He thinks we will lose them soon. We will lose them quicker if P3 if hacked. This must be a major concern.¹⁰*

8
9
10 **1. With the World's Most Infamous Hackers on its Payroll, NDS was able to Dictate When its Access Cards Would be Hacked, and Thus Could Make Additional Monies from its Customers by Selling ECMs and Ultimately Doing Expensive Card Swaps**

11
12
13 77. On or about July 11, 1997, an NDS Memorandum, concerning
14 Tarnovsky's and Kommerling's employment with NDS as two of their best
15 hackers, NDS's control over them and its desire to have Kommerling continue to
16 engage in satellite piracy, states:

17
18 *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.*

19
20
21
22
23 *. . . 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*

24
25
26 ¹⁰ Here again NDS acknowledges the fact that it was on the verge of losing one of its largest clients – DirecTV – and that drastic measures were needed to prevent such a loss. However, rather than improve the quality of its encryption technology, NDS opted to continue with its conspiracy to effectuate, and facilitate others in effectuating, a wide-spread compromise of Plaintiffs' security system to 'level the playing field' in an illegal anti-competitive manner.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9
10 **c. NDS and Tarnovsky Designed and Built the "Stinger"**
11 **that NDS, Tarnovsky, and Menard Used to Control**
12 **and Monopolize the Sales and Distribution of the**
13 **unlawfully reprogrammed Access Cards over the**
14 **Internet.**

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

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

25
26 ¹¹ As a result of Tarnovsky's December 2000 postings, satellite pirates and software
27 engineers around the world were then able to design and build their own card
28 reprogrammers thereby exacerbating the piracy of Plaintiffs' satellite television
transmission signal.

1 distribution network from potential RCMP raids.

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

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

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

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

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

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

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

- 19 a. to sell Pirated EchoStar Access Cards and other circumvention or
20 signal theft devices designed to enable users to illegally modify or alter
21 EchoStar Access Cards and/or Plaintiffs’ Security System that permit
22 unauthorized access to DISH Network programming services;
- 23 b. to perform the service (for a fee) of altering EchoStar Access Cards for
24 members of the public who submit the EchoStar Access Cards through
25 the mail;
- 26 c. to purchase EchoStar Access Cards from members of the public,
27 presumably to permit alteration and resale of the Pirated EchoStar
28 Access Cards for unauthorized access to DISH Network programming
services; and

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

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

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

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

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

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

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

1 software codes and “fixes” via the Internet that were used to circumvent Plaintiffs’
2 ECMs.

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

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

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

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