

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

JAMES A. DiBOISE, State Bar No. 083296
ELIZABETH M. SAUNDERS, State Bar No. 138249
ALEXANDER MACGILLIVRAY, State Bar No. 212770
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

C02-01178
CASE NO.

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

Plaintiffs,

v.

NDS GROUP PLC, NDS AMERICAS, INC.,

Defendants.

**COMPLAINT FOR UNFAIR
COMPETITION, COPYRIGHT
INFRINGEMENT, VIOLATION OF
THE DIGITAL MILLENIUM
COPYRIGHT ACT, TORTIOUS
INTERFERENCE, CONSPIRACY
AND VIOLATION OF THE
RACKETEER INFLUENCED AND
CORRUPT ORGANIZATIONS ACT**

JURY TRIAL DEMANDED

Plaintiffs Groupe Canal+ S.A. ("Groupe Canal+"), Canal+ Technologies S.A. ("C+ Technologies") and Canal+ Technologies, Inc. ("Canal+ USA") (Plaintiffs collectively referred to as "Canal+" or "Plaintiffs") allege on personal knowledge as to their own acts and on information and belief as to the acts of others:

INTRODUCTION

1. Canal+ seeks redress in this action for the damage caused by its competitor, NDS. Through the calculated expenditure of millions of dollars for specialized equipment and other

ORIGINAL
FILED

MAR 11 '02

RICHARD J. ...
U.S. DISTRICT COURT
NO. DIST. OF CALIF.

1 resources, NDS sabotaged C+ Technologies' previously unbroken security system for access to
2 digital television signals. In apparent disregard for both the law and its own reputation, NDS
3 caused the development of counterfeit "smart cards", permitting a theft of digital television on a
4 massive scale. Canal+ estimates that Defendants' illegal conduct has caused it harm in excess of
5 \$1,000,000,000.

6 2. C+ Technologies designs and sells systems used by pay television operators
7 around the world to control access to their copyrighted and proprietary broadcast signals. The
8 safety of those signals depends upon the security schemes adopted and implemented by Canal+.
9 Digital television providers and content providers fear the unauthorized interception of the digital
10 television signal because it deprives them of revenue, increases the costs to paying customers
11 and may permit the unauthorized digital copying of copyrighted works for illegal distribution.
12 Canal+ has implemented some of the strongest security measures that exist today in its smart
13 cards used to control access to digital television signals. Until the events described in this
14 complaint, Canal+'s security measures to protect and control access to digital television signals
15 had not been circumvented and its systems had not been cracked or counterfeited.

16 3. Published papers on the protection of access to scrambled digital television
17 signals suggest that extremely secure methods of protecting access to such signals can be
18 achieved at an appropriate price from all but the most sophisticated and well-funded efforts.
19 Indeed, Canal+'s security measures were more than adequate until March 1999 when its smart
20 card software code was copied and published on a web site called "DR7.com." After the
21 publication of that code, counterfeit Canal+ smart cards began to appear in the market. Since the
22 appearance of these counterfeit cards, Canal+ established that the publication of the Canal+ code
23 on the DR7 website has permitted counterfeiters to emulate or evade the security measures built
24 into the smart cards. The ability to circumvent these technological security measures spawned a
25 proliferation of the supply of counterfeit Canal+ smart cards and the existence of these cards has
26 caused great damage to Canal+ and the system operators who depend on its services.

27 4. After the publication of its software code on the DR7 website, Canal+ spent time
28 trying to determine how its code was stolen and who did it. Shockingly, Canal+'s investigation

1 led it to NDS. NDS devoted its substantial corporate resources to sabotage C+ Technologies'
2 technological security measures engineered into its smart cards -- a sophisticated and well-funded
3 effort that does not exist at the level of fly by night operators selling counterfeit cards at news
4 kiosks and over the Internet.

5 5. Competition should be about fair contests for customers, not "cloak and dagger"
6 operations aimed at undermining a competitor's products and services. NDS's actions
7 undermine fair competition and endanger the future of digital television. By this action, Canal+
8 seeks compensation for these wrongs and to stop NDS from similar sabotage in the future.

9 THE PARTIES

10 6. Groupe Canal+ S.A. is a corporation existing under the laws of France, with its
11 principal place of business in Paris, France. Groupe Canal+ is a media company that produces
12 films and television programming. Groupe Canal+ is the leading European producer of pay
13 television premium and sports/entertainment channels broadcast in 11 countries. Groupe Canal+
14 is also the leading European pay television operator.

15 7. Canal+ Technologies S.A. is a corporation existing under the laws of France, with
16 its principal place of business in Paris, France. C+ Technologies is one of the world's leading
17 providers of advanced software technologies that enable television network operators to deliver
18 secure programs and interactive services over digital television networks through set-top boxes.
19 These products include conditional access technology on cards that contain highly specialized
20 microchips with advanced software and encryption algorithms. These cards, commonly referred
21 to as "smart cards," limit access to digital pay television programs to lawful subscribers who pay
22 for it.

23 8. Canal+ Technologies, Inc. is a corporation existing under the laws of the State of
24 California, with its principal place of business in Cupertino, California. Canal+ USA sells and
25 markets C+ Technologies' conditional access software in the United States.

26 9. Defendant NDS Group plc ("NDS") is a corporation existing under the laws of
27 the United Kingdom with its principal place of business in Staines, Middlesex, United Kingdom.
28 NDS is a supplier of conditional access software and interactive systems on smart cards for the

1 secure delivery of entertainment and information to television set-top boxes. NDS directly
2 competes with Canal+ in this market.

3 10. Defendant NDS Americas, Inc. is a corporation existing under the laws of
4 Delaware with its principal place of business in Newport Beach, California. NDS Americas
5 performs sales, customer support, marketing functions and smart card processing for NDS. NDS
6 Americas and NDS representatives undertook significant acts in California to perpetrate the harm
7 described herein and but for those actions the harm caused to Canal+ would not have occurred.

8 JURISDICTION AND VENUE

9 11. This Court has jurisdiction over the subject matter of this Complaint pursuant to
10 28 U.S.C. §§ 1331 and 1338 due to the claims brought pursuant to 17 U.S.C. §§ 101 *et seq.* and
11 18 U.S.C §§ 1962(a), (c) and (d). This Court has supplemental jurisdiction over the remaining
12 claims pursuant to 28 U.S.C. § 1367.

13 12. Personal jurisdiction and venue in this Court are proper pursuant to 28 U.S.C.
14 §§ 1391 and 1400 and 18 U.S.C § 1965 because defendants transact business and are found in
15 this District.

16 INTRADISTRICT ASSIGNMENT

17 13. Pursuant to Local Rule 3-2(d), assignment to the San Jose Division of the U.S.
18 District Court for the Northern District of California is appropriate because Canal+'s business
19 was injured in Cupertino and elsewhere in Santa Clara County, which is a substantial basis
20 giving rise to the claims in this complaint.

21 FACTUAL BACKGROUND

22 C+ Technologies' Smart Card Technology

23 14. Even with the rise of the Internet, the television remains the most common and
24 widely used source of information and entertainment in the world today. Due to the popularity
25 of television worldwide, the television industry has constantly looked for ways to improve the
26 viewer's experience. Canal+ is at the forefront of these efforts. In recent years, Canal+ has
27 focused on developing and providing digital interactive television.

1 15. Using compression techniques and other technological advances, digital television
2 allows network operators to deliver more channels, better picture quality, improved security and
3 a wide range of interactive services that are unavailable over television using traditional analog
4 signals. To introduce the advances of digital technology to the analog television sets most
5 consumers own today, television network operators deploy digital set-top boxes, as well as smart
6 cards to be used with them, that convert the incoming digital television signal to an analog signal
7 that the television can process and display. The performance and security of digital set-top boxes
8 with smart cards are critical competitive factors in the digital broadcast industry.

9 16. C+ Technologies sold its first systems of advanced software technologies to
10 enable and secure digital interactive television through set-top boxes in 1996. These systems are
11 found in two basic products. C+ Technologies' MediaHighway interactivity software enables
12 network operators to enhance the television viewing experience with an extensive range of
13 interactive services. C+ Technologies' MediaGuard conditional access software enables network
14 operators to manage and control delivery of pay television content and provides a secure
15 platform for interactive transactions. ("Conditional access" is the term used to describe products
16 that control and secure access to digital television signals.) The MediaHighway and MediaGuard
17 software systems can be implemented together or separately in combination with software from
18 other providers. The MediaGuard conditional access product is at the center of this controversy.

19 17. Digital pay television broadcasts are encrypted to control access to the digital
20 content so that only customers who properly pay for digital television can view the offered
21 programs. This payment is particularly crucial because digital pay television content, like cable
22 content, is very often provided without commercials, and the revenue associated with it comes
23 from subscribers. A key component in C+ Technologies' MediaGuard conditional access system
24 is its smart card. A smart card, inserted into a subscriber's set-top box, deciphers access
25 messages and provides the deciphering keys needed by the set-top box to descramble the
26 broadcast stream. If the smart card authorizes viewing, it provides the set-top box with the keys
27 necessary to descramble the digital television content. This fundamental encryption/decryption
28 software is meant to ensure digital television delivery only to those entitled to receive it.

1 18. C+ Technologies has spent over \$35 million developing its MediaGuard
2 conditional access product. The MediaGuard product consists of a software suite run by the
3 television network operator on its originating server, software embedded in set top boxes, and
4 MediaGuard smart cards which are inserted into set top boxes to decipher digital television
5 signals. The software for the MediaGuard smart cards is produced by C+ Technologies under
6 strict security, and C+ Technologies devotes substantial time, money and effort to protect the
7 confidentiality of the software code it has developed for the microchips on its smart cards. These
8 efforts include, for example, requiring all C+ Technologies' employees to undertake strict
9 confidentiality obligations, limiting the number of people with access to the software code,
10 restricting access to the manufacturing facilities where the cards are customized, requiring sub-
11 contractors to agree to security measures as stringent as those implemented within C+
12 Technologies and maintaining the code on a secure stand-alone computer not connected to a
13 network. C+ Technologies also took extensive measures to protect the code on its smart cards
14 from attack. Before the events described in this Complaint, C+ Technologies' security measures
15 had never been invaded nor had the security measures used to protect the code on the cards ever
16 been circumvented.

17 **Smart Card Counterfeiting**

18 19. Counterfeit digital television smart cards represent a serious threat to the growth
19 of the digital television industry. Network operators and content providers depend on
20 subscription payments to generate revenues to cover their large costs for broadcasting
21 infrastructure, basic programming and producing content. Counterfeiting leads to loss of
22 revenue for content providers and to less funds available for development of content and the
23 deployment of new technology. This leads to reduction in the amount of content provided and
24 higher prices for paying customers.

25 20. C+ Technologies invested large sums of money and extensive human resources to
26 protect the design and contents of its smart cards. For example, C+ Technologies restricted the
27 number of people working on its smart card software code, used only one computer to develop
28 the code, completely isolated that computer from any networks and secured all backups of the

1 code in a locked safe. Once written to the smart cards, the code was protected by obfuscation
2 methods among the most advanced in the industry. These technical measures were designed to
3 obscure the information on the cards and to resist known methods used by software pirates to
4 access and read the software stored on the cards.

5 21. From the time the first C+ Technologies smart card was introduced on the market
6 in 1996 until the events described herein, the security and technical measures implemented by
7 C+ Technologies successfully protected C+ Technologies' smart cards. In late 1999, however,
8 counterfeit C+ Technologies smart cards began to emerge on the market and since that time have
9 severely and negatively impacted Canal+'s digital television business. Canal+ recently
10 uncovered evidence that its MediaGuard smart card was subjected to extensive sabotage efforts
11 by NDS that led to the production of the counterfeit C+ Technologies smart cards.

12 **NDS Cracked C+ Technologies' Smart Cards And Facilitated Counterfeiters**

13 22. The facts leading up to the widespread dissemination of counterfeit C+
14 Technologies smart cards reveal an intentional pattern of illegal conduct by NDS with its
15 ultimate aim being extensive damage to Canal+.

16 23. To accomplish its scheme, NDS obtained C+ Technologies' smart cards and sent
17 them to an NDS laboratory in Israel for analysis. At this facility, NDS had acquired and
18 assembled the costly equipment needed to conduct invasive attacks on smart cards. NDS
19 dedicated a team of software and hardware engineers at this laboratory to a special project –
20 carrying out the invasion of C+ Technologies' smart cards.

21 24. By the end of 1998 the NDS team in Israel had successfully extracted the software
22 stored on the C+ Technologies smart card through electrical and optical examination of the
23 protected internal software code of the card using expensive machinery designed and operated to
24 defeat C+ Technologies' protective measures. In early 1999, NDS used the results of this
25 invasive attack to download the UserROM software from the smart card. The UserROM is the
26 portion of the memory of a smart card which is necessary to control access to the digital stream.
27 The NDS team also created a digital archive file named "SECAROM.ZIP" containing a copy of
28 the UserROM portion of the C+ Technologies MediaGuard smart card.

1 25. NDS then took steps to have C+ Technologies' UserROM code published so that
2 counterfeiters could exploit it to develop counterfeit smart cards and thereby provide NDS with
3 an advantage in securing digital television operator contracts. NDS transmitted the
4 SECAROM.ZIP file to NDS Americas, Inc. in California with instructions that it be published on
5 the Internet so that the C+ Technologies MediaGuard UserROM code would be freely available
6 to anyone who wanted to use it to produce counterfeit C+ Technologies smart cards. NDS
7 Americas, Inc. transmitted the code from California to Al Menart, the operator of the website
8 known as "DR7.com." On March 26, 1999, DR7 published C+ Technologies' code on its
9 website.

10 26. In late 1999, counterfeit C+ Technologies smart cards began to appear on the
11 market. These cards were produced after publication of the C+ Technologies MediaGuard
12 UserROM and contained a perfect replica of the complex encryption table NDS extracted
13 through its invasive attack and caused to be published on DR7.com. Use of that encryption table
14 made the counterfeit cards work. By September 2000, the Italian market was flooded with the
15 cheap counterfeit cards and they were also proliferating in other markets. These cards are sold to
16 consumers from different retail outlets depending on the country. In some markets, consumers
17 have as ready access to the counterfeit cards as to legitimate ones. In all cases, the counterfeit
18 cards could not have existed but for the publication of the MediaGuard UserROM on the DR7
19 website, especially its complex encryption table which is embedded in all counterfeit cards and
20 enables the cards to circumvent the security measures implemented by C+ Technologies.

21 27. Through the introduction of and facilitation of the production of counterfeit C+
22 Technologies smart cards, NDS hoped to drive a wedge between Canal+ and its customers to
23 adversely impact Canal+'s business and promote NDS's own competitive position. NDS's
24 unlawful scheme succeeded. Canal+ has lost subscribers and now faces claims from client
25 television operators for financial compensation and other remedies due to their losses caused by
26 the theft of programming through counterfeit smart cards.

Harm To Canal+ From NDS's Publication of C+ Technologies Code

1
2 28. C+ Technologies has spent substantial time and money developing
3 countermeasures to combat each type of pirate smart card that resulted from the publication
4 caused by NDS. These countermeasures are created by a team of C+ Technologies engineers
5 and then tested and broadcast by the digital television operators to stop unlawful television
6 viewing by counterfeit card consumers. The countermeasures, however, are quickly made
7 obsolete by new versions of software for the counterfeit cards that pirates make available after
8 analyzing the countermeasures. Counterfeiters are able to quickly and effectively respond to
9 each new countermeasure because they have access to the UserROM code published on
10 DR7.com. C+ Technologies cannot stop this counterfeiting without implementing a fundamental
11 change in the design of the smart card. At enormous expense, C+ Technologies is currently
12 developing a new smart card design and will soon transition its existing network to the new
13 design. This transition will be time consuming and expensive because each and every legitimate
14 smart card will have to be exchanged.

15 29. The mass production of counterfeit C+ Technologies smart cards has damaged not
16 only Groupe Canal+'s direct revenue through its digital television operators, but has also hurt the
17 sales efforts of C+ Technologies and Canal+ USA. Conditional access system competitors,
18 especially NDS, use the existence of counterfeit C+ Technologies cards as a competitive weapon
19 in the sales process among content providers and system operators. For example, Canal+ has
20 encountered competitors, including NDS, pointing out to customers and potential customers in
21 the United States and elsewhere throughout the world, the breach of C+ Technologies' security
22 schemes as evidence that Canal+ cannot guarantee the integrity of its systems.

23 30. As a result of the counterfeiting, Canal+ has lost sales opportunities and has lost
24 customers to its competitors. NDS has also used the counterfeiting to attempt to disrupt
25 Canal+'s relationships with existing customers.

26 31. Another loss occasioned by NDS to Groupe Canal+ is the loss of pay per view
27 subscriptions. One common type of counterfeit access is a modification of a legitimate smart
28 card. These cards, commonly referred to as "MOSC" cards (*i.e.* "Modified Official Smart

1 Cards”), are legitimate cards, sometimes with valid basic subscriptions, that have been altered so
2 they grant their owners rights that they have not purchased. Some MOSC cards grant free access
3 to upgraded packages or to every subscription channel; others have a number of pay per view
4 television “credits” for which the owner has not paid. These cards did not exist before the
5 publication on DR7.com and but for that publication, they would not have been produced. The
6 widespread use of MOSCs has caused Groupe Canal+ and pay television operators from the
7 Canal+ group to lose revenues from premium programs.

8 32. Canal+ has been and continues to be harmed by counterfeit C+ Technologies
9 smart cards in the market. Canal+ has uncovered the origin of the counterfeit cards, and the facts
10 as set forth herein show that NDS and NDS Americas, Inc. are responsible for this harm.

11 33. Canal+ has been harmed by the unlawful acts of Defendants described herein in
12 excess of \$1 billion.

13 **COUNT I**

14 **(Unfair Competition, Cal. Bus. & Prof. Code § 17200, *et seq.*)**

15 34. Plaintiffs repeat and reallege each and every allegation set forth in paragraph 1
16 through 33.

17 35. Defendants have engaged in unfair competition in violation of the California
18 Business and Professions Code Sections 17200 *et seq.*, causing injury to Plaintiffs, including
19 Canal+ USA’s business, in Santa Clara County and elsewhere throughout California and the
20 world. Defendants willfully, unlawfully, according to a plan, and with the intention of harming
21 Plaintiffs, acquired C+ Technologies’ MediaGuard smart cards, hired engineers to teach them
22 how to violate those cards, and acquired expensive equipment to assist them in cracking the
23 smart cards for the purpose of extracting and copying C+ Technologies’ proprietary software
24 code. After transferring the code to NDS Americas, Inc. in California, Defendants caused it to
25 be disseminated it over the Internet to facilitate further copying leading to the production of
26 counterfeit C+ Technologies smart cards, all to the detriment of Canal+’s business and its
27 reputation among its customers and in the industry. This conduct constitutes an unlawful, unfair
28

1 and fraudulent business act or practice within the meaning of California Business and
2 Professions Code Section 17200 *et seq.*

3 36. Defendants' invasive attack of C+ Technologies' smart cards, copying of C+
4 Technologies' software code and dissemination of such code publicly was intentional and done
5 for the wrongful purpose of inhibiting Plaintiffs' competitive positions in the digital television
6 industry and unfairly benefiting Defendants. As a direct and proximate result of Defendants'
7 violations of California Business and Professions Code Section 17200 *et seq.*, Defendants have
8 been unjustly enriched at Plaintiffs' expense, and Plaintiffs are entitled to an accounting and
9 restitution in an amount to be determined at trial.

10 37. As a direct and proximate result of Defendants' violations of California Business
11 and Professions Code Section 17200 *et seq.*, Plaintiffs have suffered and will continue to suffer
12 irreparable harm, including but not limited to harm to their business reputations and goodwill.
13 Therefore, Plaintiffs' remedy at law is not adequate. Complete protection of Plaintiffs' rights
14 must include an injunction prohibiting Defendants from taking any steps to contribute to the
15 copying of any C+ Technologies' software code or any steps to reverse engineer or otherwise
16 violate the security measures on any C+ Technologies smart card, as well as all other remedies
17 available.

18 **COUNT II**

19 **(Common Law Unfair Competition)**

20 38. Plaintiffs repeat and reallege each and every allegation set forth in paragraph 1
21 through 37.

22 39. Plaintiffs and Defendants directly compete in the digital television and conditional
23 access smart card markets.

24 40. Defendants willfully, deliberately, according to a plan, and with the intention of
25 harming Plaintiffs, acquired C+ Technologies MediaGuard smart cards, hired engineers to teach
26 them how to violate those cards, acquired expensive equipment to assist them in cracking the
27 smart cards for the purpose of extracting and copying C+ Technologies' proprietary software
28 code and disseminating it over the Internet to facilitate further copying leading to the production

1 of counterfeit C+ Technologies smart cards, all to the detriment of Plaintiffs' reputations among
2 their customers and in the industry.

3 41. Defendants' invasive attack of C+ Technologies' smart cards, copying of C+
4 Technologies' software code and dissemination of such code publicly was intentional and done
5 for the wrongful purpose of inhibiting Plaintiffs' competitive position in the digital television
6 industry and unfairly benefiting Defendants' competitive position. As a result, Defendants have
7 engaged and continue to engage in unfair competition in violation of common law.

8 42. Defendants' wrongful acts have directly and proximately harmed Plaintiffs in an
9 amount to be determined at trial. In addition, Plaintiffs' remedy at law is not adequate.
10 Complete protection of Plaintiffs' rights must include an injunction prohibiting Defendants from
11 taking any steps to contribute to the copying of any of C+ Technologies' software code or any
12 steps to reverse engineer or otherwise violate the security measures on any C+ Technologies'
13 smart card, as well as all other remedies available.

14 **COUNT III**

15 **(Direct Copyright Infringement -- 17 U.S.C. § 101 *et seq.*)**

16 43. Plaintiffs repeat and reallege each and every allegation set forth in paragraphs 1
17 through 42.

18 44. C+ Technologies' MediaGuard UserROM software code embodies original and
19 creative authorship. C+ Technologies has devoted thousands of engineering-hours to design and
20 develop this software code. The software code, including but not limited to its "MediaGuard
21 UserROM software code for ST Chips," source code and encryption substitution table, contains a
22 substantial amount of wholly original expression and is copyrightable subject matter under the
23 laws of the United States.

24 45. C+ Technologies owns or is joint owner of the copyright to the "MediaGuard
25 UserROM software code for ST Chips" at issue in this complaint by virtue of its own creative
26 authorship of the program.

27 46. C+ Technologies has complied in all respects with the provisions of 17 U.S.C.
28 Section 101 *et seq.*, and all other laws governing copyright to secure copyright in the

1 “MediaGuard UserROM software code for ST Chips.” C+ Technologies application for
2 registration of these copyrights was submitted on February 12, 2002.

3 47. C+ Technologies has expended substantial amounts of time and resources for
4 research and development in order to improve and update the “MediaGuard UserROM software
5 code for ST Chips” and it is a substantial source of revenue for C+ Technologies.

6 48. Defendants’ reproduction, preparation of a derivative work, importation and
7 distribution of C+ Technologies’ MediaGuard UserROM code infringes C+ Technologies’
8 copyrights in its MediaGuard smart cards.

9 49. Defendants’ production of C+ Technologies’ MediaGuard UserROM in a
10 different form, creates an unauthorized derivative work and thereby infringes C+ Technologies’
11 copyrights in its MediaGuard smart cards.

12 50. Since Defendants authorized the infringement, Defendants are directly liable for
13 the infringement. Defendants’ direct copyright infringement has been and continues to be
14 willful.

15 51. The result of the aforesaid conduct of Defendants has been and will continue to be
16 to deprive C+ Technologies of goodwill, to injure C+ Technologies’ relationships with its actual
17 prospective customers, and to impose substantial expense on C+ Technologies to counteract the
18 aforesaid conduct. Defendants have also been unjustly enriched by their infringement.

19 52. Defendants’ conduct has directly and proximately caused damages to C+
20 Technologies in an amount to be proven at trial. In addition, C+ Technologies’ remedy at law is
21 not adequate. Complete protection of C+ Technologies’ rights must include an injunction
22 prohibiting Defendants from contributing to any acts of copying any C+ Technologies smart card
23 software code, as well as all other remedies available.

24 **COUNT IV**

25 **(Contributory Copyright Infringement – 17 U.S.C. § 101 *et seq.*)**

26 53. Plaintiffs repeat and reallege each and every allegation set forth in paragraphs 1
27 through 52.

28

1 67. C+ Technologies has contracts with digital television operators in countries
2 throughout Europe including the United Kingdom, France, Spain, Poland and Italy, as well as in
3 Malaysia, and potential customers in the United States. NDS knew or should have known about
4 the existence of these contracts. These operators have lost revenues because of the piracy of C+
5 Technologies smart cards. Consequently, C+ Technologies faces claims from these operators for
6 their lost revenues. This disruption of C+ Technologies' contracts with such operators has been
7 a direct result of Defendants' acts alleged herein and constitutes tortuous interference with
8 contract.

9 68. Plaintiffs have beneficial economic relationships with existing customers for pay
10 television services as well as for the MediaGuard system and component smart cards, and
11 Plaintiffs seek to continue their relationships with existing customers and at the same time gain
12 new customers in the digital broadcast market. Defendants compete in the same market as
13 Plaintiffs for the same customers. Defendants are aware of the network operators who have
14 purchased services and products from Plaintiffs and those who might so purchase. Defendants'
15 actions disrupting these relationships constitute tortuous interference with economic advantage.

16 69. Defendants deliberately took the actions set forth in this Complaint, including
17 cracking C+ Technologies' smart carts and facilitating the dissemination of C+ Technologies'
18 code for the primary purpose of disrupting Plaintiffs' contracts, relationships with existing
19 customers and relationships with potential customers by casting doubt on the security of C+
20 Technologies' smart card technology.

21 70. Plaintiffs' contracts, relationships with existing customers, and relationships with
22 potential customers it has negotiated with, have been harmed by the existence of pirated C+
23 Technologies smart cards in the market. Plaintiffs' customers do not receive payment if smart
24 cards that allow access to content with subscription exist in the market. Customers are thereby
25 deterred by the existence of counterfeit smart cards from purchasing or continuing to purchase
26 C+ Technologies' MediaHighway or MediaGuard products and generally from pursuing business
27 relationships with Plaintiffs.

1 71. Defendants' wrongful acts have directly and proximately harmed Plaintiffs in an
2 amount to be determined at trial. Defendants committed these tortious acts with deliberate and
3 actual malice, ill-will, and oppression in conscious disregard of Plaintiffs' legal rights.

4 **COUNT VII**

5 **(Civil Conspiracy)**

6 72. Plaintiffs repeat and reallege each and every allegation set forth in paragraphs 1
7 through 71.

8 73. Defendants NDS and NDS Americas knowingly and willfully conspired together
9 and with DR7, Al Menart and third party manufacturers and sellers of counterfeit smart cards to
10 (a) promote the manufacture and public distribution of counterfeit smart cards that allow for the
11 theft of services protected by C+ Technologies' security measures; and (b) undermine public
12 confidence in C+ Technologies' security measures.

13 74. Defendants NDS and NDS Americas, and later DR7, Al Menart, and third party
14 manufacturers and sellers of counterfeit smart cards, agreed to do and did the unlawful acts and
15 things herein alleged pursuant to and in furtherance of this conspiracy. The principal overt acts in
16 furtherance of the conspiracy were the transport and distribution of C+ Technologies' Media
17 Guard's UserROM code.

18 75. In addition, Defendants NDS and NDS Americas ratified and adopted the acts of
19 DR7 and Al Menart, the operator of DR7.com, by seeking their participation and assistance in
20 the conspiracy and by facilitating such participation and assistance.

21 76. The conspiracy remains operative today as entities continue to manufacture and
22 distribute counterfeit smart cards to enable the theft of services protected by C+ Technologies'
23 security measures.

24 77. As a direct and proximate result of defendants' participation in this conspiracy
25 and wrongful acts in furtherance thereof, Plaintiffs have been damaged in an amount to be
26 proven at trial.
27
28

1 78. Defendants committed these wrongful acts willfully and with the intent to cause
2 injury to Plaintiffs. Defendants acted with deliberate and actual malice, ill-will and oppression in
3 conscious disregard of Plaintiffs' legal rights.

4 COUNT VIII

5 (Violation of 18 U.S.C. §§ 1962 (a), (c), and (d) – RICO)

6 79. Plaintiffs repeat and reallege each and every allegation set forth in paragraphs 1
7 through 78.

8 80. Defendants wrongful conduct constitutes a pattern of “racketeering activity”
9 as defined by 18 USC Section 1961. Specifically, the defendants have committed at least the
10 following predicate acts: (i) criminal copyright infringement in violation of 17 U.S.C. Section
11 506(a) and 18 U.S.C. Section 2319; (ii) misconduct in connection with access devices in
12 violation of 18 U.S.C. Section 1029; and (iii) wire fraud in violation of 18 U.S.C Section 1343.

13 81. Defendants' criminal copyright infringement, in violation of 17 U.S.C. Section
14 506 and 18 U.S.C. Section 2319 is established by Defendants willful infringement of Canal+'s
15 copyrighted work to obtain commercial advantage and financial gain. Defendants committed
16 this willful infringement by knowingly making and distributing unauthorized copies of the
17 SECAROM.ZIP file. Defendants made unauthorized copies on at least three occasions: (i) on
18 NDS' mail server located in the United States upon receipt of the email message containing the
19 file or otherwise downloading the file; (ii) on the computer equipment of each individual to
20 whom the file was transferred; and (iii) on an NDS computer for electronic transfer to the
21 operator of DR7.com. These willful infringements affected and continue to affect interstate and
22 foreign commerce.

23 82. Defendants also violated 18 U.S.C. Section 1029 which prohibits certain activities
24 regarding “access devices,” including any card, code, account number, or other means of
25 accessing an account which can be used to obtain anything of value.

26 83. Defendants knowingly produced, trafficked in, controlled, and possessed “device
27 making equipment” – that is, any equipment, mechanism or impression designed or primarily
28 used for making an access device or counterfeit access device. By this conduct, Defendants

1 intended to deceive and defraud Plaintiffs and their customers through the creation and public
2 distribution of counterfeit smart cards that would falsely indicate that users of the cards were
3 authorized to receive certain digital television programming. Defendants' conduct constitutes a
4 violation of 18 U.S.C. Section 1029(a)(4). Such conduct has affected and continues to affect
5 interstate and foreign commerce.

6 84. Defendants also violated 18 U.S.C. Section 1029(b)(2) through their participation
7 in a conspiracy with Al Menart, DR7 and manufacturers and sellers of counterfeit smart cards.
8 Parties to this conspiracy (including Defendants) committed, and acted in furtherance of,
9 violations of 18 U.S.C. Section 1029(a)(1-6). The violations that Defendants conspired to
10 commit and acted to further have affected and continue to affect interstate and foreign
11 commerce.

12 85. Defendants also engaged in wire fraud in violation of 18 U.S.C. Section 1343.
13 Such violation is established by Defendants' transmission, by means of interstate or foreign
14 commerce, of an email or file containing a copy of the file SECAROM.ZIP. Such transmissions
15 were part of Defendants' scheme to deceive and defraud Plaintiffs and their customers through
16 the creation and public distribution of counterfeit smart cards that would falsely indicate that
17 users of the cards were authorized to receive certain digital television programming. Each such
18 electronic transmission was made or caused to be made to execute and further this scheme, and
19 was made or caused to be made with the specific intent to deceive and defraud Plaintiffs and
20 their customers. Defendants' violations of 18 U.S.C. Section 1343 have affected and continue to
21 affect interstate and foreign commerce.

22 86. There is a relationship between Defendants' violations of 18 U.S.C Section 2319,
23 1029 and 1343 as the violations have similar purposes, results, participants, victims, and methods
24 of commission. Defendants' repeated violations of 18 U.S.C. Sections 2319, 1029(b)(2), and
25 1343 thus amount to a pattern of related criminal and racketeering activity. There is a threat of
26 repetition of such acts, causing further harm to Plaintiffs and their customers and to
27 manufacturers of legitimate smart cards. This threat is particularly serious given the imminent
28 introduction of C+ Technologies' new smart cards and Defendants' enormous investment of time

1 and resources into destroying the security of C+ Technologies' existing conditional access
2 system.

3 87. Defendants have received income derived, directly or indirectly, from the pattern
4 of racketeering activity herein alleged, by creating for NDS an unfair competitive advantage,
5 leading to purchases from NDS that would not otherwise have been made. Defendants have
6 used, directly or indirectly, part of such income in the operation of an enterprise, NDS, which is
7 engaged in activities that affect interstate and foreign commerce. Defendants have thus violated
8 18 U.S.C. Section 1962(a).

9 88. Additionally, in 1999 and after, in the state of California and elsewhere,
10 defendants, along with Al Menart, the operator of DR7.com, were associated in fact with an
11 enterprise engaged in, and the activities of which affected, interstate and foreign commerce.
12 That enterprise was organized, supervised and directed by NDS. Through their participation in
13 the enterprise, Defendants caused the enterprise to acquire and publish the C+ Technologies'
14 Media Guard UserROM code to promote the creation and public distribution of counterfeit smart
15 cards. In violation of 18 U.S.C. 1962(c), Defendants directly and indirectly conducted and
16 participated in the conduct of such enterprise's affairs through the pattern of racketeering activity
17 described above.

18 89. Defendants violated 18 U.S.C. Section 1962(d) by conspiring to violate 18 U.S.C.
19 Section 1962(a) and (c). Defendants agreed to engage in conduct in violation of 18 U.S.C.
20 Section 1962(a) and (c) and formed, knowingly joined, and operated a conspiracy to engage in
21 such conduct. Each defendant committed and agreed to the commission of two or more of the
22 predicate offenses described above as part of its participation in the affairs of the illicit
23 enterprise.

24 90. Defendants' conduct in violation of 18 U.S.C. Sections 1962(a), (c), and (d) has
25 directly and proximately caused damages to Plaintiffs in their business and property, including
26 injury to Plaintiffs' ability to compete by reason of the unfair advantage Defendants gained by
27 their racketeering activity, in an amount to be proven at trial. Pursuant to 18 U.S.C. Section
28

1 1964(c), Plaintiffs are entitled to treble damages and to the costs of this suit, including Plaintiffs'
2 reasonable attorney's fees.

3 **PRAYER FOR RELIEF**

4 WHEREFORE, Plaintiffs pray for judgment in their favor as follows:

- 5 (a) awarding injunctive relief to Plaintiffs prohibiting Defendants from contributing
- 6 to any acts of copying any of C+ Technologies' software code and prohibiting
- 7 Defendants from taking any steps to reverse engineer or otherwise violate the
- 8 security measures on any C+ Technologies smart card;
- 9 (b) awarding damages for all injuries suffered as a result of Defendants' unlawful
- 10 conduct;
- 11 (c) awarding treble damages pursuant to 18 U.S.C. Section 1964(c);
- 12 (d) awarding an accounting and restitution in an amount to be determined at trial;
- 13 (e) awarding exemplary damages in an amount to be determined at trial;
- 14 (f) awarding pre-judgment interest in an amount to be determined at trial;
- 15 (g) awarding attorneys' fees and costs;
- 16 (h) awarding such other relief as the Court may deem just and proper.

17
18 Dated: March 11, 2002.

WILSON, SONSINI, GOODRICH & ROSATI

19
20 By: 
James A. DiBoise

21
22 Attorneys for Plaintiffs
23 GROUPE CANAL+ S.A., CANAL+
24 TECHNOLOGIES S.A. and CANAL+
25 TECHNOLOGIES, INC.