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

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

Plaintiffs,

v.

NDS GROUP PLC, NDS AMERICAS, INC.,

Defendants.

CASE NO. C02-01178 EDL

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

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

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

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

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

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

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

THE PARTIES

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

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

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

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

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

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

JURISDICTION AND VENUE

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

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

INTRADISTRICT ASSIGNMENT

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

FACTUAL BACKGROUND

C+ Technologies' Smart Card Technology

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

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

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

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

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

Smart Card Counterfeiting

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

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

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

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

NDS Cracked C+ Technologies' Smart Cards And Facilitated Counterfeiters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT I

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

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

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

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

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

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

COUNT II

(Common Law Unfair Competition)

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

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

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

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

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

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

COUNT III

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

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

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

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

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

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

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

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

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

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

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

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

COUNT IV

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

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

54. The incorporation of C+ Technologies' MediaGuard UserROM code in counterfeit smart cards constitutes an unauthorized copy, an unauthorized derivative work and unauthorized distribution and thereby infringes C+ Technologies' copyrights in its MediaGuard smart cards.

55. In creating and distributing the SECAROM.ZIP file, Defendants had knowledge of and substantially participated in the infringement of C+ Technologies' copyrights in its MediaGuard smart cards. Defendants are thus contributorily liable for this copyright infringement. Defendants' contributory copyright infringement has been and continues to be willful.

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

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

COUNT V

(Violation of DMCA – 17 U.S.C. § 1201(a)(2))

58. Plaintiffs repeat and reallege each and every allegation set forth in paragraphs 1 through 57.

59. Defendants invaded and attacked C+ Technologies' smart cards and enabled the publication of C+ Technologies' smart card software code specifically to circumvent the protections provided by C+ Technologies in those cards. The counterfeit cards that exist on the market and cause great harm to Plaintiffs were created as a result of a painstaking and entirely unauthorized process of invasive attack of C+ Technologies' smart cards to reveal the card's security measures and create the means to circumvent them.

60. C+ Technologies' MediaGuard smart cards are technological measures that are part of a deciphering system that effectively controls access to copyrighted works including television programming, movies and other pay per view events.

61. Defendants produced, imported into the United States, offered to the public, provided and trafficked in a technology, or part thereof, consisting of a ZIP archive named "SECAROM.ZIP", containing the MediaGuard UserROM and a file detailing the memory addresses of different components of the MediaGuard smart card.

62. This technology was designed and produced for the primary purpose of defeating the MediaGuard smart card's access control of copyrighted works, including digital television content.

63. The SECAROM.ZIP product has no commercially significant purpose or use other than circumventing the MediaGuard smart card's access control of copyrighted works, including digital television content. The SECAROM.ZIP product was published on a web site, DR7.com, devoted to circumventing digital television access controls, after it had been supplied by Defendants to the DR7 webmaster.

64. Defendants' actions violate Section 1201(a)(2) of the Digital Millennium Copyright Act ("DMCA"). Defendants' acts constituting DMCA violations have been and continue to be performed without the permission, license or consent of Plaintiffs.

65. Defendants' conduct has directly and proximately caused damages to Plaintiffs in an amount to be proven at trial. In addition, Plaintiffs' remedy at law is not adequate. Complete protection of Plaintiffs' rights must include an injunction prohibiting Defendants from taking any steps to reverse engineer or otherwise violate the security measures on C+ Technologies' smart cards, as well as all other remedies available.

COUNT VI

(Tortious Interference)

66. Plaintiffs repeat and reallege each and every allegation set forth in paragraphs 1 through 65.

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

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

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

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

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

COUNT VII

(Civil Conspiracy)

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

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

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

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

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

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

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

COUNT VIII

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

(a) awarding injunctive relief to Plaintiffs prohibiting Defendants from contributing to any acts of copying any of C+ Technologies' software code and prohibiting Defendants from taking any steps to reverse engineer or otherwise violate the security measures on any C+ Technologies smart card;

(b) awarding damages for all injuries suffered as a result of Defendants' unlawful conduct;

(c) awarding treble damages pursuant to 18 U.S.C. Section 1964(c);

(d) awarding an accounting and restitution in an amount to be determined at trial;

(e) awarding exemplary damages in an amount to be determined at trial;

(f) awarding pre-judgment interest in an amount to be determined at trial;

(g) awarding attorneys' fees and costs;

(h) awarding such other relief as the Court may deem just and proper.

Dated: March 11, 2002.

WILSON, SONSINI, GOODRICH & ROSATI

By: _____
James A. DiBoise

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