JAMES A. DiBOISE, State Bar No. 083296
ELIZABETH M. SAUNDERS, State Bar No. 138249
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

SAN FRANCISCO DIVISION

GROUPE CANAL+ S.A., CANAL+ TECHNOLOGIES, S.A., CANAL+ TECHNOLOGIES, INC., Plaintiffs, v. NDS GROUP PLC, NDS AMERICAS, INC., Defendants.	CASE NO.: C02-01178 VRW **DECLARATION OF JAN SAGGIORI IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED DISCOVERY AND TO PRESERVE DOCUMENTS AND THINGS** Date: April 18, 2002 Time: 2:00 p.m. Place: Courtroom 6, 17th Floor

Je soussigné Jan Saggiori, déclare ce qui suit :

1. Je suis employé par la société SSS Llc, basée à Genève, en Suisse. SSS Llc fournit des services de consulting à Canal+ dans le domaine d'accès conditionnel pour la télévision numérique.

2. Je connais Chris Tarnovsky depuis le milieu des années 90 et nous avons échangé différents email ayant trait à la télévision numérique et aux mesures de sécurité mises en œuvre pour protéger les signaux. J'ai connu Chris à travaers internet, et un ggroupe appelé « TV-Crypt ». Le groupe « TV-Crypt » était géré par Markus Kuhn quand il était étudiant à l'université d'Erlangen en Alllemagne. Lorsqu'il vivait en Allemagne, Chris et moi avons échangé des E-mail et des logiciels cooncernant les systèmes D2MAC-Eurocrypt (Canal+/TV1000) et Videocrypt (Sky/Filmnet). Chris est rentré aux Etats-Unis et nous avons continué à correspondre par E-mail. Chris commença à étudier les système Videoguard (version P1) utilisé par DirecTV aux Etats-Unis pour protéger l'accès à ses signaux satellites. Chris me demanda du code source que j'avais écrit et qui concernait l'algorithme de cryptage « DES » et les tables associées.

3. En 1997, Chris me contacta et me demanda de le mettre en contact avec des personnes susceptibles d'analyser des cartes à puce. J'ai présenté à Chris Vesselin Ivanov Nedeltchev (« Vesco ») et ai donné à Chris le numéro de téléphone de Vesco. Vesco est un ingénieur que j'ai rencontré à Genève et qui avait étudié les cartes à puce et leur systèmes de sécurité. J'ai également rencontré Vesco en mi 2001 à Genève quand il m'a contacté pour aborder en particulier des questions relatives à la sécurité du cryptage de systèmes de contrôle d'accès ; à cette époque, je compris que Vesco travaillait directement pour Reuven Hasak de NDS.

4.Très rapidement après sa publication sur le site web DR7, je fus informé qu'il était possible de télécharger à partir du site DR7 le code de la carte à puce de Canal+. Je téléchargeai ce code de la carte à puce à partir du site DR7 et examinai le code binaire ainsi que les fichiers textes inclus. Le document texte indiquait que le code de l'EEPROM avait été perdu lors du processus d'extraction mais précisait que le reste des données de la ROM utilisateur était présent dans le

fichier. J'examinai le code binaire et déterminai que le code présent à partir de l'adresse N°2000 était manquant.

5. Sachant que Chris Tarnovski connaissait Al Ménart parce que je les avait présentés en 1996 et sachant qu'Al Ménart était le gestionnaire du site DR7, je demandai à Chris s'il pouvait obtenir d'Al Ménart le code présent à partir de l'adresse N°2000. Par un échange d'Email, Chris m'envoya un fichier binaire de 8 Kilo Octets qui contenait, m'assurait-il, le code réclamé extrait de la carte à puce Canal+. Sont joints en annexe de cette présente déclaration, une copie de l' Email reçu de Chris Tarnovski (qui utilisait le pseudonyme « Arthur von Neumann » ou « Von ») en Annexe A et le code binaire transmis par cet Email en annexe B.

6. Plus tard en 1999, après que Chris m'eût rendu visite à Genève, nous discutâmes la possibilité d'obtenir plus d'information concernant le composant Thomson utilisé dans les cartes à puce Canal+. Chris m'envoya par Email un fichier qui contenait le manuel utilisateur du composant Thomson. La page de garde du document que j'ai reçu de Chris est joint en annexe C de cette présente déclaration. Le document reçu est une copie d'un manuel utilisateur confidentiel de Thomson qu'il n'est possible d'obtenir de Thomson qu'à travers un strict accord de confidentialité.

Je déclare, sous risque de poursuites selon les lois des Etats Unis d'Amérique, que ma présente déclaration est exacte et sincère.

Signé : 8 Avril 2002, à Paris, France.

/s/Jan Saggiori
Jan Saggiori