

**UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF FLORIDA  
TAMPA DIVISION**

DISH NETWORK L.L.C. et al.,	)	Case No. 8:11-cv-00308-JSM-EAJ
	)	
Plaintiffs,	)	
	)	
v.	)	
	)	
I.E. ENTERTAINMENT, INC. et al.	)	
	)	
Defendants.	)	
	/	

---

**FINAL JUDGMENT AND PERMANENT INJUNCTION**

1. Plaintiffs brought this action against defendants I.E. Entertainment, Inc., Ian Jones, and Eric Johnson, individually and d/b/a abadss.com (collectively, “Defendants”), for unlawfully manufacturing, distributing, and otherwise trafficking in tools, software, devices, components, and technologies intended to facilitate the illegal and unauthorized reception and decryption of DISH Network’s satellite television programming.

2. DISH Network is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a Direct Broadcast Satellite (“DBS”) system. DISH Network uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services (“Programming”) to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price).

3. To provide customers with a variety of programming channels, DISH Network continues to contract with and purchases the distribution rights of copyrighted programming from providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other content providers, including without limitation HBO, ESPN, SHOW Time, Cinemax and Disney among others.

4. Because DISH Network generates revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain the distribution rights for programming is dependent upon preventing the unauthorized reception of DISH Network programming signals, all of DISH Network's video channels, except for certain promotional channels, are digitally secured and encrypted.

5. Plaintiffs protect their DISH Network Programming from unauthorized viewing by using a management and security system ("Security System"), which serves two interrelated functions: (1) subscriber-management—allowing DISH Network to "turn on" or "turn off" Programming that a customer ordered, cancelled, or changed; and (2) encryption—preventing individuals or entities who have not purchased DISH Network Programming from viewing it.

6. The Security System is comprised of two parts. First, DISH Network encrypts (electronically scrambles) its satellite signals using proprietary technology provided by NagraStar. Essentially, NagraStar provides DISH Network with "smart cards" ("Access Cards") that contain a microprocessor component that functions as a security computer to a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"). These Access Cards and related encryption technology are utilized in the satellite receivers that customers either purchase or lease. Second, the DNASP uses a complex encryption system that is combined with a Digital Video Broadcasting ("DVB") scrambler/encoding system to effectively protect and encrypt DISH Network Programming.

7. Defendants violated 17 U.S.C. § 1201(a)(2) and 47 U.S.C. § 605(e)(4) by distributing and otherwise trafficking in tools, software, devices, components, and technologies that are primarily designed to circumvent and defeat Plaintiffs' Security System and ultimately facilitate the unauthorized reception of Plaintiffs' encrypted satellite signals and copyrighted DISH Network Programming. Defendants acknowledge and admit that the tools, software, and devices that they distributed on [www.abadss.com](http://www.abadss.com) were primarily designed, marketed, and used to facilitate piracy of DISH Network programming.

## **II. FINAL JUDGMENT & PERMANENT INJUNCTION**

Upon stipulation by the Parties, the Court hereby **ORDERS** and **ADJUDGES** as follows:

(1) Defendants and anyone acting in active concert or participation with, or at the direction or control of Defendants are hereby **PERMANENTLY ENJOINED** from:

(a) offering to the public, providing, or otherwise trafficking in any satellite television receivers or set-top-boxes, software, firmware, 8PSK boards, or any other device, component, or technology, or part thereof, through any means including Internet Key Sharing (also known as Control Word Sharing), that:

(i) is primarily designed or produced for the purpose of circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform;

(ii) has only a limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform; or

(iii) is marketed by any Defendant and/or others acting in concert with any Defendant for use in circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform;

(b) assembling, modifying, selling, importing, and/or distributing any satellite television receivers, set-top-boxes, software, firmware, 8PSK boards, or other device, technology or part thereof knowing or having reason to know that such device, technology or part thereof is primarily of assistance in the unauthorized decryption of direct-to-home satellite services through any means including Internet Key Sharing (also known as Control Word Sharing);

(c) intercepting Plaintiffs' satellite transmissions without Plaintiffs' authorization through any means including Internet Key Sharing (also known as Control Word Sharing);

(d) assisting others in intercepting Plaintiffs' satellite transmissions without Plaintiffs' authorization through any means including Internet Key Sharing (also known as Control Word Sharing);

(e) testing, analyzing, reverse engineering, manipulating or otherwise extracting codes or other technological information or data from Plaintiffs' satellite television receivers, access cards, data stream or any other part or component of Plaintiffs' Security System or other technology used to gain access to DISH Network Programming including through the use of Internet Key Sharing (also known as Control Word Sharing); and

(f) operating any website or URL that markets, promotes, distributes, or provides any information or discussion forums related to the products, devices, technology, codes, software, hardware, firmware, dongles, or components thereof which Defendants are permanently enjoined from manufacturing, promoting, distributing or trafficking in pursuant to section (1)(a)-(e) above of this Final Judgment and Permanent Injunction.

(2) This Permanent Injunction takes effect immediately.

(3) Should any Defendant breach any part of this Final Judgment or Permanent Injunction, that Defendant shall be subject to damages up to the amount of \$110,000 for each

such breach or violation, which is the maximum statutory damage permitted per violation under 47 U.S.C. § 605(e)(3)(C)(i)-(ii). For purposes of assessing damages under this section, each “device, product, file, technology or part or component thereof” that is distributed by Defendants or others acting in active participation or concert with Defendants in violation of this Final Judgment and Permanent Injunction shall constitute a separate and discrete violation. In the case of any software, firmware, or other file distributed or posted by Defendants or others acting in active participation or concert with Defendants, each time that software, firmware or other file is downloaded by an end-user shall constitute a separate and discrete “violation” for purposes of quantifying damages set forth in this section. In the case of Defendants’ use of Internet Key Sharing (“IKS”) products or services to gain unauthorized access to DISH Network Programming, each decryption key or “control work” used by Defendants or Defendants’ equipment to descramble DISH Network Programming shall constitute a separate and discrete “violation” for purposes of quantifying damages set forth in this section.

(4) The Court further ORDERS judgment in favor of Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C. and NagraStar LLC on each of Plaintiffs’ claims under 17 U.S.C. § 1201, 47 U.S.C. § 605, and Vicarious Liability (Counts 1-3 in Plaintiffs’ First Amended Complaint) as to Defendants.

(5) The Court awards Plaintiffs statutory damages in the amount of \$8,993,600.00 as to Defendant I.E. Entertainment on Plaintiffs’ claim under 17 U.S.C. §1201(a)(2);


(6) The Court retains jurisdiction over this action for the purposes of enforcing this Final Judgment and Permanent Injunction and adjudicating any disputes regarding the Parties’ underlying settlement agreement, including but not limited to disputes regarding the enforcement or scope of the settlement agreement.

(7) Each of the Parties is to bear its own costs and attorney’s fees.

(8) This is a final judgment. Any and all relief not expressly granted herein is denied.

It is so ORDERED.

SIGNED and ENTERED this 14 day of Feb., 2012.

  
\_\_\_\_\_  
JAMES S. MOODY, JR.  
UNITED STATES DISTRICT JUDGE