UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE

DISH NETWORK LLC, ECHOSTAR TECHNOLOGIES LLC, and NAGRASTAR LLC,	)	
Plaintiffs,	)	
v.	)	No.: 3:15-CV-492-TAV-HBG
LESTER BARNABY,	)	
Defendant.	)	

MEMORANDUM OPINION

This civil action is before the Court on plaintiffs' Motion for Default Judgment [Doc. 6]. Plaintiffs move for entry of a judgment by default against defendant pursuant to Rule 55(b)(2) of the Federal Rules of Civil Procedure for failure to answer the complaint or otherwise defend this action. The Court has carefully considered the record as well as the relevant law, and for the reasons discussed herein, the Court will grant plaintiffs' motion.

I. Background

Plaintiff DISH Network LLC ("DISH") is a multi-channel video provider that delivers video, audio, and data services to approximately fourteen-million subscribers throughout the United States via a direct broadcast satellite system [Doc. 1 ¶ 9]. DISH uses high-powered satellites to broadcast entertainment services to consumers who have been authorized to receive such services after payment of a fee [*Id.* ¶ 10]. It contracts for and purchases the distribution rights for most of the programming available for broadcast

[*Id.* ¶ 11]. The programming DISH broadcasts are copyrighted and DISH has the authority of the copyright holders to protect these works from unauthorized reception and viewing [*Id.* ¶ 12].

The programming is digitized, compressed, and then scrambled prior to being transmitted to multiple satellites [*Id.* ¶ 13]. The satellites relay the encrypted signal and DISH subscribers, who have the necessary equipment, receive the signals [*Id.*]. Plaintiff EchoStar Technologies LLC ("EchoStar") provides receivers, dish antenna, and other digital equipment for the DISH system [*Id.* ¶ 14]. Plaintiff NagraStar LLC ("NagraStar") provides security technologies [*Id.*]. The security measures are encryption-based technologies that descramble the satellite signal [*Id.* ¶¶ 16–18]. These measures prevent unauthorized users from viewing the programming [*Id.*]

A new form of piracy has emerged called "Internet key sharing," or "IKS," that can circumvent this system by use of passcodes [*Id.* ¶¶ 21–24]. NFusion Private Server ("NFPS") is a subscription-based IKS service, whereby members purchase the service to receive DISH's encrypted satellite broadcasts of programing without authorization [*Id.* ¶ 25]. Plaintiffs received records showing that defendant purchased at least 220 passcodes to the NFPS service [Docs. 8-1, 8-2].[1] These passcode are primarily designed and produced for circumventing the DISH system and have no commercially significant purpose other than to do so [Doc. 1 ¶ 32]. Plaintiffs assert that defendant re-sold certain

[1] The Court notes that plaintiffs alleged in the complaint that defendant purchased at least 160 passcodes [Doc. 1 ¶ 26]. In connection with their request for damages, however, plaintiffs provided additional evidence showing that he purchased at least 220 passcodes [Docs. 8-1, 8-2].

IKS passwords that he purchased [*Id.* ¶ 27]. They allege that defendant intended for his IKS passwords to be used in the unauthorized decryption of plaintiffs' satellite signal, and knew or at least should have known they were used primarily in this unlawful manner [*Id.* ¶¶ 34, 38–39]. Defendant and his customers received the benefit of viewing DISH programming without purchasing a subscription [*Id.* ¶¶ 27–28].

Plaintiffs filed this action on November 2, 2015, alleging violations of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201, *et seq.*, and the Federal Communications Act ("FCA"), 47 U.S.C. § 605, *et seq.* [Doc. 1 ¶ 5].[2] Defendant failed to respond to the complaint or otherwise defend this action despite being properly served [Docs. 2, 3]. On February 9, 2016, plaintiffs applied for the Clerk's entry of default [Doc. 4], and on March 3, 2016, the Clerk of Court entered default [Doc. 5].

II. Analysis

Rule 55 of the Federal Rules of Civil Procedure contemplates a two-step process for obtaining a default judgment against a defendant who has failed to plead or otherwise defend. First, pursuant to Rule 55(a), a plaintiff must request from the Clerk of Court an entry of default, describing the particulars of the defendant's failure to plead or otherwise defend. If default is entered by the Clerk, the plaintiff must then move the Court for entry of default judgment pursuant to Rule 55(b). The determination of whether a motion for default judgment should be granted is committed to "the sound discretion of the court." *In re Irby*, 337 B.R. 293, 294 (Bankr. N.D. Ohio 2005) (applying Federal Rule of

[2] Plaintiffs also alleged violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511, *et seq.*, but do not move for default judgment on that basis.

Bankruptcy Procedure 7055, which incorporates Federal Rule of Civil Procedure 55).

Once default has been entered, "the complaint's factual allegations regarding liability are taken as true." *Bogard v. Nat'l Credit Consultants*, No. 1:12 CV 02509, 2013 WL 2209154, at *3 (N.D. Ohio May 20, 2013); *see also Nat'l Satellite Sports, Inc. v. Mosley Entm't, Inc.*, No. 01-CV-74510-DT, 2002 WL 1303039, at *3 (E.D. Mich. May 21, 2002) ("For a default judgment, well-pleaded factual allegations are sufficient to establish a defendant's liability."). The Court must, however, determine whether the facts alleged in the complaint "are sufficient to state a claim for relief as to each cause of action for which [plaintiffs] seek[] default judgment." *J & J Sports Prods., Inc. v. Rodriguez*, No. 1:08-CV-1350, 2008 WL 5083149, at *1 (N.D. Ohio Nov. 25, 2008); *see also Harrison v. Bailey*, 107 F.3d 870, 1997 WL 49955, at *1 (6th Cir. Feb. 6, 1997) ("Default judgments would not have been proper due to the failure to state a claim against these defendants."); *Vinton v. CG's Prep Kitchen & Café*, No. 1:09-CV-707, 2010 WL 748221, at *1 (W.D. Mich. Mar. 2, 2010) ("A default judgment therefore cannot stand on a complaint that fails to state a claim."). Furthermore, although the allegations in the complaint pertaining to liability are taken as true, "the amount of damages must be proven." *Bogard*, 2013 WL 2209154, at *3.

Plaintiffs move for default judgment as to their claims under the DMCA and the FCA. The Court will first address the sufficiently of the complaint as to the claims arising out of each statute. Then, the Court will address damages.

A. Sufficiency of the Complaint as to the DCMA Claims

The DCMA addresses the circumvention of copyright protection systems. 17 U.S.C. § 1201. It prohibits trafficking in any technology, service, or part thereof that: (1) is primarily designed or produced for circumventing a technological measure that effectively controls access to a copyrighted work; (2) has only limited commercial purpose or use other than circumventing a technological measure that effectively controls access to a copyrighted work; or (3) is marketed for use in circumventing a technological measure that effectively controls access to a copyrighted work. *Id.* § 1201(a)(2). Circumventing technological measures, as defined in the DCMA, "means to descramble a scrambled work, to decrypt an encrypted work, or to otherwise avoid, bypass, remove, deactivate, or impair a technological measure." *Id.* § 1201(a)(3)(A).

Courts have previously held that encryption-based security systems, such as plaintiffs' system, constitute an effective access control measure for purposes of the DMCA. *See DISH Network L.L.C. v. Sonicview USA, Inc.*, No. 09-CV-1553-L(WVG), 2012 WL 1965279, at *8 (S.D. Cal. May 31, 2012); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) (holding that security measures based on "encryption or scrambling" are effective for purposes of the DMCA). In addition, courts have held that the DCMA applies to various piracy instruments including passcodes. *DISH Network LLC v. DiMarco*, No. 2:11-CV-01962, 2012 WL 917812, at *5 (D. Nev. Mar. 14, 2012) (finding the DMCA applicable to the distribution of passwords used to access IKS servers); *DISH Network LLC v. Dillion*, No. 12-CV-157

BTM(NLS), 2012 WL 368214, at *3-4 (S.D. Cal. Feb. 3, 2012) (finding that the DMCA and the FCA apply to piracy-enabling software files); *see also Actuate Corp. v. IBM Corp.*, No. C-09- 05892 JCS, 2010 WL 1340519, at *9 (N.D. Cal. Apr. 5, 2010) (holding the "unauthorized distribution of passwords and usernames avoids and bypasses a technological measure in violation of section[] 1201(a)(2)").

Plaintiffs have adequately plead a claim for relief under § 1201(a)(2) of the DMCA. In their complaint, they state that defendant purchased and sold the IKS passcodes, that these passcodes are primarily designed to circumvent the plaintiffs' security system, and that they have no commercially significant purpose other than to do so. Altogether, the allegations in plaintiffs' complaint, which are accepted as true, establish that defendant trafficked in IKS passcodes in violation of the DMCA. As such, plaintiffs are entitled to default judgment as to their DMCA claims.

B. Sufficiency of the Complaint as to the FCA Claims

Section 605(e)(4) of the FCA is similar to § 1201(a)(2) of the DCMA. That section of the FCA by makes it unlawful for any person to import or distribute any device or equipment while "knowing or having reason to know" that the device or equipment "is primarily of assistance in the unauthorized decryption of . . . direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a)." 47 U.S.C. § 605(e)(4). Furthermore, subsection (a) provides that, "[n]o person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by

radio and use such communication . . . for his own benefit or for the benefit of another not entitled thereto." *Id.* § 605(a).

Courts have held that plaintiffs' satellite television broadcasts are direct-to-home satellite services for purposes of § 605(e)(4), and protected radio communications under § 605(a). *See DirecTV, Inc. v. Webb*, 545 F.3d 837, 844 (9th Cir. 2008); *DirecTV, Inc. v. Huynh*, 503 F.3d 847, 852–53 (9th Cir. 2007); *Sonicview USA*, 2012 WL 1965279, at *10. The FCA also applies to various piracy instruments including passcodes. *Dillion*, 2012 WL 368214, at *3–4 (finding that the DMCA and the FCA apply to piracy-enabling software files).

The Court also finds that plaintiffs have adequately plead a claim for relief under § 605(e)(4) of the FCA. In addition to the allegations in the complaint previously discussed in conjunction with the DMCA, plaintiffs provide that defendant knew, or at least should have known, that the codes were being primarily used in an unlawful manner. Furthermore, defendant and his customers received the benefit of viewing DISH programming without purchasing a subscription.

Having found that defendant faces liability under the DMCA and the FCA, the Court turns to the issue of relief sought. Plaintiffs seek relief in the form of statutory damages and a permanent injunction.

C. Statutory Damages

Plaintiffs are entitled to recover statutory damages for each of defendant's violations of the DMCA and FCA. *See* 17 U.S.C. § 1203(c)(3)(A) (authorizing $200 to

$2,500 per product); 47 U.S.C. §§ 605(e)(3)(C)(i)(II), (e)(4) ($10,000 to $100,000 for each product). Plaintiffs seek $1,000 for each of 220 infringing products under the DMCA.

Based on the evidence attached to plaintiffs' motion, including the declaration of Chirstopher Ross, an intelligence analyst with plaintiff NagaraStar, and the documentation provided by a confidential informant, the Court finds that defendant trafficked in at least 220 IKS Server Passcodes [Docs. 8-1, 8-2]. The Court must determine, however, whether plaintiffs are entitled to $1,000 per passcode.

District courts applying the DMCA "have wide discretion in determining the amount of statutory damages to be awarded, constrained only by the specified maxima and minima." *Echo Star Satellite LLC v. Viewtech, Inc.*, No. 07cv1273 BEN (WVW), 2011 WL 1522409, at *3 (S.D. Cal. Apr. 20, 2011) (quoting *Peer Int'l Corp. v. Pausa Records, Inc.*, 909 F.2d 1332, 1336 (9th Cir. 1990)). When determining the amount of damages to be awarded for each violation, the willfulness of the conduct and need for deterrence may be considered. *See Sony Computer Entm't Am., Inc. v. Filipiak*, 406 F. Supp. 2d 1068, 1074-75 (N.D. Cal. 2005); *Tracfone Wireless, Inc. v. SND Cellular, Inc.*, 715 F. Supp. 2d 1246, 1261-62 (S.D. Fla. 2010). In the context of § 1201(a)(2), "willful" means acting with knowledge that the product at issue is designed or used for circumvention. *See Filipiak*, 406 F. Supp. 2d at 1075 (citing *Dolman v. Agee*, 157 F.3d 708, 715 (9th Cir. 1998)).

To support the contention that they are entitled to $1,000 per passcode, plaintiffs point to the declaration of Moss which establishes that the 220 passcodes only encompass the period of 2011–2013 even though the NFPS service continued to operate after 2013 [Doc. 8-1 ¶ 5]. In addition, defendant may have purchased passcodes from persons other than the confidential informant [*Id.*]. Plaintiffs also note that the $1,000 per passcode requested is far below the top end of the DMCA's damages range. 17 U.S.C. § 1203(c)(3)(A) ($200 to $2,500 per item).

As the Court has already noted, the passcodes were designed and used to circumvent the security system. In addition, the large number of passcodes defendant purchased is evidence that he knew the passcodes were designed and used for this purpose. *See Hendrix*, 2005 WL 757562, at *6 (finding that purchasing 200 devices is evidence of knowledge). Furthermore, plaintiffs provided evidence that defendant has been purchasing piracy equipment since at least November 2011 [Docs. 8-1, 8-2]. These facts all support that defendant's actions were willful.

The Court also notes that plaintiffs are not requesting damages for defendant's violations of § 605(e)(4), which range from $10,000 to $100,000 for each product. 47 U.S.C. §§ 605(e)(3)(C)(i)(II), (e)(4). Plaintiffs are also not requesting an award of attorneys' fees or costs, which are available under the DMCA in the Court's discretion, and mandatory under the FCA. *See* 17 U.S.C. § 1203(b)(4)–(5); 47 U.S.C. § 605(e)(3)(B)(iii).

Furthermore, the Court notes that several courts have awarded statutory damages at this level. *See, e.g., DISH Network L.L.C. v. Erian*, No. 3:15-cv-01159, at Doc. 18 (M.D. Tenn.) (granting default judgment and awarding $1,000 for each violation of the DMCA); *DISH Network L.L.C. v. Bolanos*, No. CV 12-3097 DSF (OPx), 2012 WL 5896599, at *1 (C.D. Cal. Nov. 21, 2012); *Tracfone Wireless*, 715 F. Supp. 2d at 1261; *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1064 (N.D. Cal. 2010).

Accordingly, the Court finds that the $1,000 per DMCA violation requested by plaintiffs is appropriate. At $1,000 for each of the 220 passcodes, plaintiffs are entitled to damages in the amount of $220,000.

D. Permanent Injunction

Plaintiffs also request a permanent injunction pursuant to the Federal Rules of Civil Procedure and the DMCA. *See* Fed. R. Civ. P. 65; 17 U.S.C. § 1203(b)(1) ("the court . . . may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation"). In order to obtain relief in the form of a permanent injunction, a plaintiff must show the following:

> (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

eBay, Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006). The Court will address each of these factors in turn.

1. Irreparable Harm and Inadequacy of Monetary Damages

As to irreparable harm, plaintiffs have provided the declaration of Gregory Duval, the Chief Operating Officer with plaintiff NagaraStar, to support its position that they have satisfied this requirement [Doc. 8-3]. Duval's statements establish that the plaintiffs invest millions of dollars each year in security measures to protect from unauthorized viewing of programming [*Id.* ¶ 18]. Defendant's acts of trafficking in IKS passcodes undermine the investment in technology and results in the need for costly security updates [*Id.* ¶ 19]. In addition, the piracy defendant has been engaged in harms the reputation of plaintiffs and interferes with the contractual and prospective business relationships of the companies [*Id.* ¶ 20].

Furthermore, Duval's declaration establishes this type of piracy impacts plaintiffs' bottom line to an extent that cannot be fully ascertained. Plaintiffs receive approximately $84 per month from a subscriber [*Id.* ¶ 21]. Defendant and the persons that acquired passcodes from defendant enjoyed access to programing, including premium and pay-per-view channels [*Id.*]. Duval notes that determining the amount of profit lost is impracticable because the nature and extent of programming unlawfully received through use of IKS passcodes is unknown [*Id.*].

As such, plaintiffs have shown that calculating reputational damage and lost sales is inherently difficult, if not impossible, and therefore constitutes irreparable harm and establishes the inadequacy of monetary damages. *See Tom Doherty Assoc. v. Saban Entm't, Inc.*, 60 F.3d 27, 37–38 (2d Cir. 1995) (noting that "a loss of prospective

goodwill can constitute irreparable harm"); *see also Coxcom, Inc. v. Chaffee*, 536 F.3d 101, 112 (1st Cir. 2008) (granting permanent injunction and finding irreparable harm based on the relative inability to detect cable piracy and the magnitude of lost programming revenues); *DISH Network L.L.C. v. Whitcomb*, No. 11-CV-0333 W (RBB), 2011 WL 1559825, at *3 (S.D. Cal. Apr. 25, 2011) (concluding that lost profits and subscribers resulting from the sale of DISH Network piracy devices constitutes irreparable harm); *Macrovision v. Sima Prods., Corp.*, No. 05 Civ. 5587 (RO), 2006 WL 1063284, at *3 (S.D.N.Y. Apr. 20, 2006) ("If [the plaintiff] is unable to prevent the circumvention of its technology, its business goodwill will likely be eroded, and the damages flowing therefrom extremely difficult to quantify."). As such, plaintiffs have established irreparable harm and the inadequacy of monetary damages.

2. Balance of Hardships and Public Interest

The Court must also balance of hardships between plaintiffs and defendant and consider whether the public interest would be disserved by a permanent injunction. Absent an injunction, plaintiffs would be irreparably harmed as discussed herein. In contrast, should the Court issue an injunction, defendant will only suffer a loss of revenue from the sale of his infringing products—which should be given minimal weight. *See Cadence Design Sys., Inc. v. Avant! Corp.*, 125 F.3d 824, 829 (9th Cir. 1997) (finding that profits lost from the enjoined sales of infringing goods is not cognizable harm); *Triad Sys. Corp. v. Se. Express Co.*, 64 F.3d 1330, 1338 (9th Cir. 1995) ("[The defendant]

cannot complain of the harm that will befall it when properly forced to desist from its infringing activities.")

In addition, the public interest is served by enjoining activities that violate federal law. *See Whitcomb*, 2011 WL 1559825, at *4 (noting the strong public interest in the enforcement of the DMCA) (citing *Coxcom*, 536 F.3d at 112). Permanently enjoining defendant will also serve the public interest by upholding copyright protections and advancing the goal of copyright law which is to "prevent[] the misappropriation of the skills, creative energies, and resources which are invested in the protected works." *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1255 (3d Cir. 1983). In contrast, allowing defendant to continue trafficking in IKS passcodes does not benefit the public. *See Grokster*, 518 F. Supp. 2d at 1223 ("Certainly, the public does not benefit from [the defendant's] inducement of infringement.").

As such, the balance of hardships and consideration of the public interest also favor a permanent injunction. In sum, the Court finds that all factors weigh in favor of issuing a permanent injunction against defendant. The Court now turns to the terms of that injunction.

3. Terms of the Injunction

The Court has broad discretion pursuant to Federal Rule of Civil Procedure 65 "to restrain acts which are of the same type or class as unlawful acts which the court has found to have been committed or whose commission in the future, unless enjoined, may be fairly anticipated from the defendant's conduct in the past." *Orantes-Hernandez v.*

Thornburgh, 919 F.2d 549, 564 (9th Cir. 1990). Similarly, the DMCA authorizes the Court to grant a permanent injunction on such terms as it deems reasonable to prevent or restrain a violation of the statute. *See* 17 U.S.C. § 1203(b)(1).

Plaintiffs request that the Court issue the following permanent injunction:

> Defendant, and anyone acting in active concert or participation with Defendant, is hereby permanently enjoined from:
>
> - manufacturing, importing, offering to the public, providing, or otherwise trafficking in IKS Server Passcodes, any other code or password used in accessing an IKS server, and any other technology or part thereof that is used in circumventing DISH Network's security system or receiving DISH Network programming without authorization;
>
> - circumventing or assisting others in circumventing the DISH Network security system, or receiving or assisting others in receiving DISH Network's satellite signal without authorization; and
>
> - testing, analyzing, reverse engineering, manipulating, or extracting code, data, or information from DISH Network's satellite receivers, smart cards, satellite stream, or any other part or component of the DISH Network security system

[Doc. 7 pp. 11–12]. Plaintiffs further note that "[p]ermanent injunctions have been entered in similar cases on essentially the same terms" [*Id.* at 12 (citing *Sonicview USA*, 2012 WL 1965279, at *14; *Viewtech*, 2011 WL 1522409, at *4).

In the cases plaintiffs cited, however, the courts only enjoined the defendants in the action from engaging in such conduct. *See Sonicview USA*, 2012 WL 1965279, at *; *Viewtech*, 2011 WL 1522409, at *4. Here, plaintiffs ask the Court to enjoin defendant and "anyone acting in active concert or participation with Defendant" from engaging in the conduct described. The Court does not find that it is appropriate to enjoin individuals

who are not parties in this action and have not had an opportunity to properly defend themselves. The Court does, however, find that the proposed injunction is appropriate as to defendant and will permanently enjoin defendant from engaging in such action.

III. Conclusion

For the reasons discussed herein, the Court will **GRANT** plaintiffs' Motion for Default Judgment [Doc. 6]. Accordingly, judgment will be entered in favor of plaintiffs as to Count I of the complaint alleging violations of 17 U.S.C. § 1201(a)(2), and Count II of the complaint alleging violations of 47 U.S.C. § 605(e)(4). Statutory damages in the amount of $220,000 will be awarded to plaintiffs. The Court will also permanently enjoin defendant as follows:

> Defendant is hereby permanently enjoined from:
>
> - manufacturing, importing, offering to the public, providing, or otherwise trafficking in IKS Server Passcodes, any other code or password used in accessing an IKS server, and any other technology or part thereof that is used in circumventing DISH Network's security system or receiving DISH Network programming without authorization;
>
> - circumventing or assisting others in circumventing the DISH Network security system, or receiving or assisting others in receiving DISH Network's satellite signal without authorization; and
>
> - testing, analyzing, reverse engineering, manipulating, or extracting code, data, or information from DISH Network's satellite receivers, smart cards, satellite stream, or any other part or component of the DISH Network security system.

The Court retains jurisdiction over this action for the purpose of enforcing the final judgment and permanent injunction. The Clerk of Court will be **DIRECTED** to send

defendant a copy of this memorandum opinion and the contemporaneously issued order by standard first class U.S. mail to his last known address. The Clerk of Court will further be **DIRECTED** to **CLOSE** this action.

ORDER ACCORDINGLY.

s/ Thomas A. Varlan
CHIEF UNITED STATES DISTRICT JUDGE