

UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

INSTALLATION SOFTWARE TECHNOLOGIES,)	
INC. d/b/a INSTALLSHIELD SOFTWARE)	
CORPORATION,)	
)	
Plaintiff,)	No. 03 C 4502
)	
v.)	Judge Coar
)	
WISE SOLUTIONS, INC.,)	Magistrate Judge Denlow
)	
Defendant.)	

**PLAINTIFF'S MEMORANDUM IN SUPPORT
OF ITS RULE 65 MOTION FOR A TEMPORARY
RESTRAINING ORDER AND PRELIMINARY INJUNCTION**

Plaintiff, INSTALLATION SOFTWARE TECHNOLOGIES, INC. d/b/a
INSTALLSHIELD SOFTWARE CORPORATION ("InstallShield"), submits this memorandum
in support of its Rule 65 motion for a temporary restraining order and preliminary injunction,
with notice.

I. INTRODUCTION

As described in InstallShield's Verified Complaint and supporting Declarations, this
action arises out of an ongoing investigation by the United States Attorney, the Federal Bureau
of Investigation and InstallShield into defendant's long-term and ongoing criminal conduct in
using electronic espionage, on at least 903 occasions, to circumvent computer password
protections in order to acquire and use InstallShield's confidential, proprietary and trade secret
information for unfair competitive purposes. InstallShield seeks a temporary restraining order
and preliminary injunction under the Digital Millennium Copyright Act, 17 U.S.C. § 1203, the

Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), the Copyright Act, 17 U.S.C. § 502, and the Illinois Trade Secrets Act, 765 ILCS 1065/3.

II. JURISDICTION AND VENUE

This Court has original subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331, as the matter in controversy concerns defendant's violations of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201 *et seq.* ("DMCA"), the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* ("CFAA") and the Copyright Act of 1976, 17 U.S.C. §§ 101 *et seq.* ("Copyright Act"). Additionally, this Court has original subject matter jurisdiction over plaintiff's claim under the Illinois Trade Secrets Act, 765 ILCS 1065/1 *et seq.* ("ITSA") pursuant to 28 U.S.C. § 1332(a)(2) because the amount in controversy exceeds \$75,000, exclusive of interest and costs, and diversity of citizenship exists between plaintiff and defendant. *See Rexford Rand Corp. v. Ancel*, 58 F.3d 1215, 1218 (7th Cir. 1995) (in injunction litigation, amount in controversy, for diversity jurisdiction purposes, is measured by value of rights sought to be protected). Plaintiff InstallShield is a Illinois corporation with its principal place of business in Schaumburg, Illinois. Defendant Wise is a Michigan corporation with its principal place of business in Plymouth, Michigan.

Venue is proper in this district under 28 U.S.C. § 1391, as plaintiff resides in this district and because the events or omissions giving rise to the claims herein occurred in substantial part in this district. Furthermore, the harm from defendant's violations of the DMCA, the CFAA, the Copyright Act and the ITSA, has been sustained in this district.

III. CHOICE OF LAW

A federal court exercising diversity jurisdiction normally must look to the choice-of-law rules of the state in which the federal court sits. *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S.

487, 496 (1941). However, the Seventh Circuit has held that the false conflict doctrine applies where there is no difference between the laws of the contact states. *Barron v. Ford Motor Co. of Canada, Ltd.*, 965 F.2d 195, 197 (7th Cir. 1992); *In re Aircrash Disaster*, 644 F.2d 594, 605 n.2 (7th Cir. 1981). Under this doctrine, the Court will generally choose the law of the forum state, in this case Illinois, in analyzing the claims presented. *International Administrators Inc. v. Life Ins. Co. of N. Am.*, 753 F.2d 1373, 1376 n.4 (7th Cir. 1985). Both the ITSA and the Michigan Trade Secret Act, MCLS § 445.1901 *et seq.*, are derived from the Uniform Trade Secrets Act. Thus, this Court should apply the ITSA under the false conflicts doctrine. The DMCA, the CFAA and the Copyright Act, as federal statutes, do not present conflicts issues.

IV. EQUITABLE RELIEF IS MANDATED BY STATUTE AND BY COMMON LAW

Under the facts described in InstallShield's Verified Complaint, the Court should issue an injunction on statutory grounds. Generally, "in an action for a statutory injunction, once a violation has been demonstrated, the moving party need only show that there is a reasonable likelihood of future violations in order to obtain relief." *CSC Holdings, Inc. v. Greenleaf Electronics, Inc.*, No. 99 C 7249, 2000 U.S. Dist. LEXIS 7675, at *28 (N.D. Ill. June 1, 2000).

The temporary restraining order and preliminary injunction relief requested by InstallShield is expressly authorized by the four statutes implicated by defendant's wrongful conduct. *See* 17 U.S.C. § 1203 (under the DMCA, the "court may grant temporary and permanent injunctions"); 18 U.S.C. § 1030(g) (CFAA provides for "injunctive or other equitable relief"); 17 U.S.C. § 502 ("The Copyright Act authorizes injunctive relief in situations where it is reasonable for the purpose of restraining or preventing infringement of copyright"); 765 ILCS 1065/3 ("Actual or threatened or threatened misappropriation may be enjoined" under the ITSA).

Additionally and alternatively, Rule 65 authorizes this Court to issue a temporary restraining order and preliminary injunction based on InstallShield's showing that: (1)

InstallShield is likely to succeed on the merits; (2) InstallShield will suffer irreparable harm if an injunction is not issued; (3) InstallShield lacks an adequate remedy at law; (4) the balance of harms tips in favor of InstallShield; and (5) the public interest favors injunctive relief. *Foodcomm International v. Barry*, 328 F.3d 300, 303 (7th Cir. 2003); *Roland Machinery v. Dresser Industries*, 749 F.2d 380, 386-87 (7th Cir. 1984). This Court is to apply a “sliding scale” in evaluating these elements. *Storck USA, L.P. v. Farley Candy Co.*, 14 F.3d 311, 314 (7th Cir. 1994). Particularly in view of defendant’s long-term and repeated criminal conduct, there is a significant likelihood that in the absence of injunctive relief defendant will continue to obtain access to InstallShield’s computers or otherwise continue to disclose, use and benefit from the proprietary and confidential information it has stolen from InstallShield’s computers. As further explained below, InstallShield does not have an adequate remedy at law for its ongoing injuries and will suffer irreparable harm if injunctive relief is not granted.

V. LIKELIHOOD OF SUCCESS ON THE MERITS

Plaintiff need only show that its chances of succeeding on the merits are “better than negligible.” *Roland Machinery*, 749 F.2d at 387. As the Seventh Circuit has explained, “although a plaintiff must demonstrate some probability of success on the merits, the threshold is low.” *Brunswick Corp. v. Jones*, 784 F.2d 271, 275 (7th Cir. 1986). In this case, for the reasons that follow, InstallShield has demonstrated that its chances of succeeding on the merits are far “better than negligible,” given defendant’s blatant violations of applicable federal and state law. Even if “likelihood of success on the merits” were understood as imposing a higher burden of proof than “better than negligible,” InstallShield would still prevail, as InstallShield is virtually certain to prevail on the merits.

A. InstallShield's Claim for Violation of Digital Millennium Copyright Act

InstallShield has a likelihood of succeeding on the merits of its DMCA claim. The DMCA's anti-circumvention rule provides that "No person shall circumvent a technological measure that effectively controls access to a work protected under this title [Title 17]." 17 U.S.C. § 1201(a)(1)(A). As the court explained in *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), "Section 1201(a)(1) governs 'the act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work,' an act described by Congress as 'the electronic equivalent of breaking into a locked room in order to obtain a copy of a book.'" *Id.* at 316, *quoting* H.R. REP. No. 105-551(I), 105th Cong., 2d Sess. at 17 (1998); *see also Pearl Investments, LLC v. Standard I/O, Inc.*, No. 02-50-P-H, 2003 U.S. Dist. LEXIS 5376, at *60 (D.Me. Apr. 2, 2003) (holding that encrypted, password-protected virtual private network ("VPN") is "electronic equivalent" of locked door).

Here, InstallShield had security measures in place, including confidential passwords and usernames, designed to restrict access to the files on its computers, including its ftp server. These "technological measures" effectively controlled access to InstallShield's works because they were measures which, in the ordinary course of [their] operation, require[d] the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work" 17 U.S.C. §1201(3)(B). There can be no question that Wise "circumvented" InstallShield's technological measures when it used InstallShield's passwords and usernames to acquire access to the files on InstallShield's ftp server.

Each of the files downloaded by Wise from InstallShield's server was, at all relevant times, a "work protected" under Title 17. 17 U.S.C. § 1201(a). As stated in *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 441 (2d Cir. 2001), "work protected" as referred to in the

DMCA is equivalent to “work protected under Title 17,” meaning the Copyright Act. Pursuant to the Copyright Act, in order to qualify as a “work protected,” a work must be copyrightable, but it need not necessarily have been actually registered with the Copyright Office at the time of the infringement. *Mist-On Sys. v. Gilley’s European Tan Spa*, No. 02-C- 0038-C, 2002 U.S. Dist. Lexis 9846 (W.D. Wis. 2002); *Lakedreams v. Taylor*, 932 F.2d 1103, 1108 (5th Cir. 1991); *Apple Barrel Prods., Inc. v. Beard*, 730 F.2d 384 (5th Cir. 1984). InstallShield’s works of authorship, including its compilation of customer names and contacts, reflects more than the minimum originality required under the Copyright Act. *Mid America Title Co. v. Kirk*, 991 F.2d 417, 421 (7th Cir. 1993). Thus, all of InstallShield’s copyrightable data stolen by Wise is entitled to the protections of the DMCA.

Finally, courts have found injunctive relief to be appropriate in actions under the DMCA. *See, e.g., Corley*, 273 F.3d at 458 (injunction ordered under DMCA was not in violation of First Amendment); *In Re: Aimster Copyright Litigation*, 252 F. Supp. 2d 634, 665 (N.D. Ill. 2002) (motion for preliminary injunction granted where operating system’s users were engaged in copyright infringement). In short, InstallShield has readily demonstrated a likelihood of success on its claim under the DMCA.

B. InstallShield’s Claim for Violation of the Computer Fraud and Abuse Act

InstallShield has also demonstrated a likelihood of succeeding on the merits of its civil claim under the CFAA. InstallShield’s computers and servers are “protected computers” within the meaning of Section 1030 (e)(2)(B) of the CFAA, as they are “used in interstate or foreign commerce or communication.”

InstallShield has sufficiently demonstrated that Wise, intentionally and without authorization, obtained access to InstallShield’s protected computers in violation of 18 U.S.C. § 1030(a)(5)(B). Indeed, there can be no question that Wise systematically and intentionally

violated the CFAA at least 903 times. *See Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, No. 01-4572-Civ-MOORE, 2003 U.S. Dist. LEXIS 8717, at *153 (S.D. Fla. May 9, 2003) (finding that defendant had violated § (a)(5)(A)(ii) and (a)(5)(A)(iii) “by intentionally accessing Four Seasons’ protected computers and thereby obtaining information of value in the form of confidential customer and financial data.”).

Wise’s unauthorized access to InstallShield’s computers caused “damage” within the meaning of Section 1030 (e)(8) of the CFAA. Section 1030(e)(8) defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” As the *Four Seasons* court held, “customer information [alone] has previously been held to constitute a property interest sufficient to satisfy the damage requirement of the CFAA.” 2003 U.S. Dist. LEXIS 8717, at 153-54. Indeed, Wise’s theft of InstallShield’s 103,000 Customer Mailing List itself satisfies the CFAA’s “damage” requirement.

Wise’s violation of the CFAA also caused InstallShield to incur “loss” in excess of \$5,000. The CFAA defines “loss” as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense and any revenue lost, cost incurred, or other consequential damages incurred because of interruption in service.” 18 U.S.C. § 1030(e)(11). To be sure, as set forth in InstallShield Verified Complaint and supporting Declarations, the loss to InstallShield of responding to Wise’s illegal acts, assessing the damage, making the necessary repairs, and the revenue lost by InstallShield as a result of Wise’s actions amounts to far more than \$5,000. *See* Verified Complaint, Count I, at ¶ 70; Decl. of Viresh Bhatia at ¶ 45.

C. InstallShield's Claim for Violation of the Copyright Act of 1976

InstallShield also has a better than negligible chance of success on its copyright infringement claim. To establish copyright infringement, InstallShield must prove that it owns a valid copyright, and that defendant has committed an unauthorized copying of the original elements of the work. *Feist Publications, Inc. v. Rural T. Serv. Co., Inc.*, 499 U.S. 340, 361 (1991).

InstallShield is the owner of valid registered copyrights in each of the following works: (a) *Making Sense of Windows Installer Setups*, (b) *Getting Started with InstallShield Developer and Windows Installer Setups*, and (c) the *Administrator's Introduction to Application Repackaging and Software Development Using Windows Installer*. Wise willfully reproduced and misappropriated these copyrighted materials through its unauthorized access of InstallShield's computers. Wise's actions constitute copyright infringement in violation of the Copyright Act. Thus, InstallShield is entitled to injunctive relief under the Copyright Act. *See* 17 U.S.C. § 502.

D. InstallShield's Claim for Violation of the Illinois Trade Secrets Act

The ITSA expressly prohibits "espionage through electronic or other means." 765 ILCS 1065/2. Section 3 of the ITSA provides that "actual or threatened misappropriation may be enjoined." 765 ILCS 1065/3. *See also PepsiCo v. Redmond*, 54 F.3d 1262 (7th Cir. 1995) (affirming injunction to prevent inevitable disclosure of trade secrets); *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 880 (N.D. Ill. 2001) (granting permanent injunction based upon actual misappropriation of trade secrets); *Stampede Tool Warehouse v. May*, 272 Ill. App. 3d 580, 651 N.E.2d 209 (1st Dist. 1995) (award of injunctive relief upheld where defendants misappropriated a customer list which qualified as a trade secret under the Act).

As described in InstallShield's Verified Complaint, Wise misappropriated the following InstallShield trade secrets using espionage through electronic means: (1) InstallShield's 103,000 Customer Mailing List, (2) InstallShield's 6,000 Customer Mailing List, (3) the artwork and copy for InstallShield's "Cast Your .Net Far And Wide" advertising campaign, and (4) InstallShield's beta software.

Each of these items are "trade secrets," as defined in Section 2 of the ITSA. Section 2 of the ITSA broadly defines "trade secret" as follows:

"Trade secret" means information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

765 ILCS 1065/4.

InstallShield's 103,000 Customer Mailing List and the 6,000 Customer Mailing List are, of course, lists of "actual or potential customers" as set forth in the ITSA's definition of "trade secret." These lists were maintained by InstallShield in strict confidence, plainly have economic value by virtue of the relative secrecy, and were in fact misappropriated by Wise, as evidenced by its mailings to InstallShield's decoy addresses.

Similarly, InstallShield's "Cast Your .Net Far and Wide" advertising campaign and marketing strategy was maintained in strict confidence by InstallShield, had economic value by virtue of its relative secrecy, and was obviously misappropriated by Wise, as evidenced by Wise's preemptive "Cast Your .Net far and *Wise*" ad campaign (emphasis added).

As also described in InstallShield's Verified Complaint, InstallShield's beta software was maintained in strict confidence by InstallShield and made available only to certain customers for

testing purposes. Wise obtained access to and downloaded this beta software from InstallShield's ftp server. The beta software was for an InstallShield software product that InstallShield calls "AdminStudio 5.0." InstallShield believes that Wise opened the beta software using InstallShield's confidential passwords, thereby obtaining access to its contents. By obtaining InstallShield's beta software, Wise was able to anticipate InstallShield's the features and capabilities of InstallShield's AdminStudio 5.0 before it was released to market. This information was of obvious competitive value to Wise as evidenced by Wise's decision to call its competitive product, "PackageStudio 6.0," skipping "5.0" so as to undercut InstallShield's marketing of its new software. For these reasons, InstallShield has demonstrated a likelihood that it will succeed on its claim under the Illinois Trade Secrets Act.

VI. IRREPARABLE HARM WITH NO ADEQUATE REMEDY AT LAW

Wise's multiple violations of the DMCA, the CFAA, the Copyright Act and the ITSA have caused, and continue to cause, irreparable damage to InstallShield which cannot be adequately compensated with money damages. InstallShield's irreparable injuries include, but are not limited to: loss of customers, both potential and actual; loss of customer goodwill and loss of competitive advantage.

Damages arising from all of these injuries are impossible to fully calculate by any precise pecuniary standard. *Foodcomm International v. Barry*, 328 F.3d 300, 304-05 (7th Cir. 2003) ("not practicable to calculate damages to remedy" harm resulting from loss of customer relationship); *Cleveland Hair Clinic, Inc. v. Puig*, No. 96 C 3560, 1996 WL 691432, at *21 (N.D. Ill., Nov. 22, 1996) (holding that plaintiff's "loss of future customers and revenues, as well as its loss of good will, is an irreparable injury for which injunctive relief is appropriate"); *YourNetDating, LLC v. Mitchell*, 88 F. Supp. 2d 870, (N.D. Ill. 2000) (granting TRO in CFAA case where "the showing of irreparable harm is the damage to the goodwill of its services");

Register.Com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (granting preliminary injunction in CFAA case where found irreparable harm resulted from defendant's use of misappropriated data for marketing purposes); *Aimster*, 2002 U.S. Dist. LEXIS 17054, at *28, citing *Atari Inc. v. North Am. Philips Consumer Elec. Corp.*, 672 F.2d 607, 620 (7th Cir.), cert. denied, 459 U.S. 880, 74 L. Ed. 2d 145, 103 S. Ct. 176 (1982) (“[i]rreparable injury may normally be presumed from a showing of copyright infringement”); *Petrzilka v. Gorscak*, 199 Ill. App. 3d 120, 124-25, 556 N.E.2d 1265, 1268 (1st Dist. 1990) (granting injunction because lost profits due to the loss of potential sales are “incapable of adequate computation, and thus money damages are not an adequate remedy”); *Burt Dickens & Co. v. Bodi*, 144 Ill. App. 3d 875, 494 N.E.2d 817 (1st Dist. 1986) (no adequate remedy at law exists for stolen customer list; the proper remedy in cases of misappropriation is to enjoin the defendant from competing for the customers whose names are contained on the list). That InstallShield's losses are defendants' gains merely makes this situation that much worse and the need for injunctive relief that much greater.

VII. BALANCE OF HARMS AND PUBLIC INTEREST

The balance of harms weighs heavily in favor of granting InstallShield's request for injunctive relief. Defendants over the course of at least one year and on an almost daily basis, willfully and repeatedly engaged in criminal conduct. To the extent that Wise suffers harm from the grant of injunctive relief, such harm results solely from their willful violations of applicable federal and state law.

In balancing the prospective harms, a defendant's claim of irreparable harm rings hollow when he decides to engage in improper conduct with knowledge of the potential consequences. *Ty, Inc. v. Jones Group Inc.*, 237 F.3d 891, 903 (7th Cir. 2001). The only harm an injunction would inflict upon defendants would be to enjoin them from engaging in the criminal conduct that they have directed at InstallShield for at least one year, and from further benefiting from

their criminal conduct. Put simply, “illegal activities are not worthy of any protection.” *CSC Holdings*, 2000 U.S. Dist. LEXIS 7675, at *26. Furthermore, as the Illinois Appellate Court held in *ABC Transnational Transport, Inc. v. Aeronautics Forwarders Inc.*, 62 Ill. App. 3d 671, 682, 379 N.E.2d 1228, 1236 (1st Dist. 1978), the balance of harms analysis

is inapplicable where defendant’s ‘actions were done with full knowledge of the plaintiff’s rights and with an understanding of the consequences which might ensue.

See also Foodcomm International v. Barry, 328 F.3d 300, 305 (7th Cir. 2003) (affirming preliminary injunction even if it may have required deportation of defendants); *Horn Abbot, Ltd. v. Sarsaparilla, Ltd.*, 601 F. Supp. 360, 369 (N.D. Ill. 1984) (“Even though equitable relief will probably put [defendant] out of business, we disagree that its hardship outweighs that of Horn Abbot”); *Loewen Group Int’l, Inc. v. Haberichter*, No. 93 C 7377, 1997 U.S. Dist. LEXIS 15678, at *30 (N.D. Ill. Sept. 29, 1997) (holding that because defendant “acted with full knowledge of the potentially devastating consequences of his actions, an equity court will not protect one who knowingly and intentionally places himself in harm’s way”); *J.H. Chapman Group, Ltd. v. Chapman*, No. 95 C 7716, 1996 U.S. Dist. LEXIS 899, at *16 (N.D. Ill. Jan. 30, 1996) (harm to plaintiff would outweigh harm to defendant if injunction were not issued as plaintiff stood chance of losing customers and sales, while injunction would not “flatly prevent defendants from selling their services”); *ABC Transnational Transport, Inc. v. Aeronautics Forwarders Inc.*, 90 Ill. App. 3d 817, 832-33, 413 N.E.2d 1299, 1311 (1st Dist. 1980) (“a preliminary injunction could properly issue even if the effect would be to put [defendant] out of business as long as [plaintiff] made a sufficient showing of irreparable harm to a legitimate interest, the inadequacy of legal relief, and the likelihood of prevailing on the merits”).

Finally, the public interest weighs heavily in favor of injunctive relief preventing defendant from engaging in conduct that is unlawful and detrimental to InstallShield. *See CSC*

Holdings, 2000 U.S. Dist. LEXIS at *26 (holding that defendants illegal sales of cable television “descramblers” were “against the public interest”). Furthermore, the public has an interest in being protected from inducements to buy products that are based on stolen data, such as the “Cast Your .Net Far and *Wise*” advertising campaign, which was conceived, generated, and disseminated using data stolen from InstallShield’s computers. See *Dunkin Donuts v. Benita Corp.*, No. 97 C 2934, 1998 U.S. Dist. LEXIS 1716 at *19 (N.D. Ill. Feb. 6, 1998) (granting preliminary injunction to franchisor in Lanham Act case, holding that “[t]he public has a right not to be confused and deceived, and the right to make an informed purchase.”).

VIII. SCOPE OF INJUNCTION

In addition to a nondisclosure injunction and other equitable relief, InstallShield is seeking a prophylactic “use” injunction. A use injunction for trade secret misappropriation, including customer list theft, is proper. See *Burt Dickens & Co. v. Bodi*, 144 Ill. App. 3d 875, 885-86, 494 N.E.2d 817, 823-24 (“Since the court would have no way of knowing if defendant was using the expiration list to solicit Dickens’ accounts, it is not difficult to justify the blanket prohibition of such solicitation even if carried out with the aid of sources other than the lists.”).

InstallShield is also seeking preliminary injunctive relief in the form of the imposition of a constructive trust on all revenues obtained by the defendant as a result of its use of data stolen from InstallShield. Interlocutory relief of the same character as final relief is always permitted. See *DeBeers Consolidated Mines, Ltd. v. U.S.*, 325 U.S. 212, 220 (1945). InstallShield requests that the Court order the defendant to immediately identify all revenues it derived from its use of InstallShield’s trade secrets and other proprietary materials. This information is needed so the Court can fashion an appropriate constructive trust injunction freeze order. See *FTC v. Think Achievement Corp.*, 312 F.3d 259, 262 (7th Cir. 2003) (asset freeze is appropriate to ensure restitution to victim).

IX. THE COURT SHOULD WAIVE BOND

This Court should waive bond, or, in the alternative, set a *de minimis* bond in this case. First, this Court has the discretion to waive a bond “in appropriate circumstances.” *Wayne Chem., Inc. v. Columbus Agency Serv. Corp.*, 567 F.2d 692, 701 (7th Cir. 1977). Second, a lower bond “may be permissible” where a plaintiff demonstrates a “strong likelihood of success on the merits.” *Scherr v. Volpe*, 466 F.2d 1027, 1035 (7th Cir. 1972). Here, InstallShield has incontrovertible proof that Wise has illegally accessed its computers and misappropriated its proprietary data, thus providing an overwhelming likelihood that InstallShield will prove violations of the statutes under which it has brought this suit. Moreover, the issuance of an injunction—which, in essence, will only preclude Wise from continuing its illegal conduct—will not harm Wise. *See Smith v. Board of Election Commissioners*, 586 F. Supp. 309 (N.D. Ill. 1984) (one factor to consider in issuing a bond is harm to defendant if injunction issues).

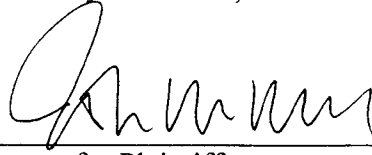
The purpose of the injunctive relief InstallShield seeks is tailored to prevent defendant from engaging in any additional unlawful acts, and to prevent defendant from continuing to wrongfully benefit from its prior unlawful acts. In no legitimate sense will defendant be “harmed” if the injunctive relief requested by InstallShield is issued. *See Lawson v. City of Kankakee*, 81 F. Supp. 2d 930, 936 (C.D. Ill. 2000) (no bond required where no harm would befall defendant where preliminary injunction issued); *Special Educ. Servs. v. RREEF Performance Partnership-I*, No. 95 C 6468, 1996 U.S. Dist. LEXIS 907, at **5-6 (N.D. Ill. Jan. 25, 1996) (no bond required because injunction would do “little or no” harm to defendant).

X. CONCLUSION

For these reasons, InstallShield’s motion for a temporary restraining order and preliminary injunction should be granted. For the Court’s convenience, InstallShield has prepared the attached draft Temporary Restraining Order.

Dated: June 30, 2003

Respectfully submitted,



Attorneys for Plaintiff,
INSTALLATION SOFTWARE
TECHNOLOGIES, INC. d/b/a INSTALLSHIELD
SOFTWARE CORPORATION

#28

William Lynch Schaller
John M. Murphy
Charles R. Topping
Hillary P. Krantz
BAKER & MCKENZIE
One Prudential Plaza
130 East Randolph Drive
Chicago, IL 60601
(312) 861-8000

CHIDOC01, 377788.1