UIC John Marshall Journal of Information Technology & Privacy Law

Volume 5
Issue 2 *Computer/Law Journal - Fall 1984*

Article 2

Fall 1984

Legal and Technical Protection Through Software Locks, 5 Computer L.J. 163 (1984)

Edward C. Saltzberg

LEGAL AND TECHNICAL PROTECTION THROUGH SOFTWARE LOCKS†

by EDWARD C. SALTZBERG*

TABLE OF CONTENTS

This Article describes some of the possible legal ramifications of the use of "software locks" by software vendors. Since the author has been unable to find any reported cases that deal specifically with the use of software locks, this is a somewhat ambitious endeavor. The lack of specific precedents is not foreign to those who practice what is commonly known as "computer law," however. It is often necessary to draw analogies to existing, non-computer-related law. This Article is an example of such an undertaking.

The legal questions surrounding the use of software locks fall into two general categories: 1) whether such devices offer legally enforceable protection for the software vendor; and 2) what the legal ramifications are regarding their misuse. After defining "software locks" and examining reasons for their use, this Article will explore some possible answers to these questions.

I. SOFTWARE LOCKS DEFINED

For the purposes of this Article, a "software lock" is a technical measure employed by a software vendor to prevent unauthorized use of the software. The most commonly used measure is one which

* Member of the Massachusetts Bar. J.D., Suffolk University Law School, 1976; M.B.A., Boston University, 1973; B.A., Boston University, 1969.

establishes an expiration date after which the program will cease to operate. For example, the date May 1, 1984 is embedded in the software. Each time the software is initialized, it checks to see if the current date is earlier than the embedded date. If so, the program will continue to operate. If not (e.g., the current date is May 2, 1984), the software either will not operate or, in a more aggressive software lock, will erase itself.[1]

This simple type of software lock can be bypassed by a user in either of two ways. First, a user may simply enter a false value for the current date, that is, a date that he knows is before the expiration date. This procedure may be difficult in cases where the subject software uses the actual current date to perform date calculations, or to print or display the actual current date in the heading of the output of the program.

The second method by which a user may bypass the expiration date is to alter the date embedded in the software itself. Typically, software is distributed in "binary code," rather than "source code" form. Source code is the actual computer program written in a language understandable to anyone who has had training in its use. On the other hand, binary code (also "executable code" or "object code") is not easily understandable by human beings. It is the product of a process whereby the source code is translated by the computer into a form which the computer can then understand, appearing to the reader as a set of "0's" and "1's." It is difficult, but not impossible, for one who is knowledgeable about the software in question to find and alter the binary code version of a software lock.

The process of decoding the expiration date software lock is simplified if the user knows exactly how the lock is implemented. Disclosing the nature of the software lock is similar to telling a car thief exactly what type of antitheft protection a particular car has. A skilled car thief, given enough time, can bypass just about any antitheft device. The disclosure of the type of protection device used greatly reduces the amount of time needed to bypass it.

A software developer who goes to the trouble of employing a software lock generally does not disclose how the lock is employed. One can surmise, however, that the software locks actually used are more sophisticated than the simple version described above. For example, the software developer may employ a procedure in which

1. A software lock that not only erases itself, but also erases or scrambles the user's data is beyond the scope of this Article. Such a lock might involve a tortious or criminal interference with the user's property. *See* MASS. GEN. LAWS ANN. ch. 93, § 42 (West 1984); ch. 266, § 30(4) (West 1970 & Supp. 1984) (proscribing misappropriation or larceny of trade secrets). *See generally* Howitt, *Of Worms and Booby Traps*, INFOWORLD, Nov. 19, 1984, at 45, 46.

the date entered by the user must be later than the date entered the last time the software was used, but earlier than the embedded expiration date. Additionally, a software lock may count the number of times the software is initialized. The developer would estimate how many times a user would initiate the program within a certain defined period of time and use that as all or part of the software lock.

Another type of software lock is one in which the computer's serial number is embedded in the software so that the software will only operate on the designated computer. The serial number software lock may be technically possible on larger computer systems, but is not readily available for personal or micro computers.

One type of copy protection that has become popular only within the past several months is fingerprinted diskettes. This is not a software lock as such, but a unique way of physically marking each diskette. The software (without the fingerprint) can still be copied, but the program will not run unless the fingerprinted diskette is physically present in the computer. In other words, the user must put the original diskette provided by the vendor in the computer; a copy of that diskette without the unique fingerprint will not execute. One must go to considerable effort to bypass the fingerprint lock, a process that may discourage the casual copier and will test the determination of the confirmed software pirate.

As time goes by, it is likely that the software industry will devise more effective techniques for guarding against unauthorized use. Meanwhile, the legal ramifications of the use of software locks ought to be considered.

II. REASONS FOR USING SOFTWARE LOCKS

The purpose of the software lock is to force the user to perform some act, usually the payment of money, to avoid the automatic shutdown of the program. Upon the performance of the act, the software vendor reinitializes the software or otherwise disables the software lock. It should be noted that although a software lock will not prevent unauthorized copying, it may prevent operation of an unauthorized copy that includes the lock.

Perhaps the most common use of software locks is with demonstration versions of software. Since most users want to try software before they buy it, many vendors offer a demonstration version for a nominal or no fee. The demonstration version can be either a limited capacity or fully featured version that is usable for a limited period of time, usually thirty days. The fully featured version is preferable, since it enables the user to experience the full power of

the software. By offering this version, however, vendors incur the risk that less scrupulous users will bypass the software lock and obtain free use of the software.

It is estimated that at least forty percent of the software in circulation is unauthorized.[2] There are several basic reasons underlying this phenomenon. First, it is extremely easy to copy software; the process takes from a few seconds to several minutes, depending on the software's volume. Software is easier to copy than videotape. While two recorders are required to copy a videotape, only one computer is required to copy software. Indeed, most vendors encourage the copying of their software for back-up purposes.[3] Second, unauthorized software copying is not as clearly perceived as a legal and ethical violation as, for example, videotape copying. Third, the economic incentive for unauthorized software copying is quite significant. A single software license generally costs at least several hundred dollars and, in many cases, thousands. Finally, it is extremely unlikely a vendor will discover those persons making unauthorized copies of its software, let alone commence litigation for what may be both civil and criminal copyright violations.

Worldwide revenues from software sales are now estimated to be $4 billion. To put that figure in perspective, worldwide revenues from the publication of books are only $9 billion.[4] By 1986, software sales are estimated to exceed $16 billion.[5] Revenue losses from the unauthorized use of software are now and will continue to be enormous. Software locks can be a critical security measure of significant economic value.

III. THE SOFTWARE LOCK AS AN ARTICLE NINE SECURITY INTEREST

Section 1-201(37) of the Uniform Commercial Code (U.C.C.) defines "security interest" as "an interest in personal property or fix-

---

2. Azzara, *Copyright Protection for Software: Court Rule Seen as Landmark*, Computer Sys. News, Sept. 12, 1983, at 10; Tyler, *Only One Per Customer*, DATAMATION, Apr. 15, 1984, at 49; *Can Software Makers Win the War against Piracy?*, BUS. WK., Apr. 30, 1984, at 108, 109.

3. *See* IBM CORP., IBM PC GUIDE TO OPERATIONS at 3-26 (1983) ("Before you begin to use your software purchase, you should . . . make a copy of the diskette we provide . . . ."); OSBORNE COMPUTER CORP., dBASE II ASSEMBLY-LANGUAGE RELATIONAL DATABASE MANAGEMENT SYSTEM VERSION 2.36 (Manual Revision 1C, Dec. 10, 1982) at 9.

4. Bigelow, *Copyrights and Computer Software—A Conference Summary*, COMPUTER L. & TAX REP., Apr. 1984, at 3 (quoting IBM's senior corporate patent counsel).

5. Rosenberg, *Software Piracy: Formulating a Plan for Protection*, COMPUTERWORLD, Sept. 12, 1983, at 149.

tures which secures payment *or* performance of an obligation" (emphasis added).

U.C.C. section 9-102 sets forth the policy and subject matter of Article Nine. It states that Article Nine applies "to any transaction (regardless of its form) which is intended to create a security interest in personal property or fixtures including goods, documents, instruments, general intangibles, chattel paper or accounts . . . ."

Based on sections 1-201(37) and 9-102, it appears that a software lock falls squarely within Article Nine, provided that it is intended to secure the payment of money *or* the performance of an obligation.

Appendix A provides a sample contract between a licensor and licensee regarding the use of computer software, fictionally known as "GENDOC."[6] Paragraph 7 of the agreement sets forth five different conditions that can trip the software lock. The conditions concern the fulfillment of the licensee's obligations under the License Agreement or other agreements between the parties, including nonpayment of money due.

Is the GENDOC License Agreement a "security agreement"? U.C.C. section 9-105(1)(L) defines a "security agreement" as "an agreement which creates or provides for a security interest . . . ." There is no requirement that the agreement be labelled as such.[7] Whether a particular document or transaction creates a security interest depends upon the intent of the parties.[8] Under U.C.C. section 9-203, a security interest is enforceable against the debtor or third parties if the security agreement is signed by the debtor and contains a description of the collateral. Since the GENDOC License Agreement would be signed by the debtor and describes the collateral, it appears to meet the Article Nine requirements for a security agreement.[9]

---

6. *See infra* p. 173.

7. Peterson v. Ziegler, 39 Ill. App. 3d 379, 350 N.E.2d 356 (1976) (application for certificate of title describing collateral and signed by debtor found to constitute a security agreement), *overruled on other grounds*, Dwyer v. Cooksville Grain Co., 117 Ill. App. 3d 1001, 454 N.E.2d 357 (1983).

8. *See* Foley Machine Co. v. John T. Brady Co., 62 Misc. 2d 777, 310 N.Y.S.2d 49 (N.Y. Sup. Ct. 1970).

9. An interesting question arises where a vendor provides a user with a demonstration version of the software under a "blisterpack" license. A blisterpack license is a unilateral agreement from the vendor which essentially says the user agrees to the terms of the license agreement if the user tears open the plastic blisterpack covering the software diskette. Because such a license agreement is not physically signed by the user, it may not satisfy the requirements of section 9-203. Furthermore, it does not appear that the action of opening the blisterpack would fall within the definition of "signature" provided in U.C.C. § 1-201(39), which "includes any symbol executed or adopted by a party with a present intention to authenticate a writing." Opening the

What is the collateral? U.C.C. section 9-105(c) states, " 'collateral' means the property subject to a security interest. . . ." In the GENDOC License Agreement, the collateral is the non-exclusive and non-transferable license to use the GENDOC. While a license is property in which a valid security interest may lie,[10] the question may be asked whether a license to use software is the type of property that can be used to secure an interest.

It is clear that if software falls in the categories of either "goods" or "general intangibles," then it is the type of property to which a security interest may lie. Distinguishing between software as goods and software as general intangibles may be an interesting academic exercise, but the distinction is not necessary to answer the threshold question of whether a software lock falls within Article Nine.[11] Nevertheless, the distinction may have some relevance to the questions of when a security interest attaches, proper jurisdiction, proper methods of perfection, and proper methods of realizing on software that is collateral.[12] The distinction may also be critically important in determining a secured party's rights under U.C.C. section 9-503.[13]

Certain transactions are excluded from Article Nine by U.C.C. section 9-104. One of those exclusions relates to a security interest subject to any statute of the United States to the extent that such statute governs the rights of parties to, and third parties affected by, transactions in particular types of property. Since software now clearly appears to be copyrightable subject matter,[14] and copyright is governed exclusively by federal law,[15] software may be excluded from Article Nine under this provision. It is not clear, however, that federal copyright law preempts all of the Article Nine provisions

---

blisterpack may not rise to the level of creating a symbol intended to authenticate a writing.

For an analysis of the enforceability of blisterpack licenses, see Reynolds, *The Self-Executing License: A Legal Fiction*, 2 COMPUTER L. REP. 549 (1984).

10. Bogus v. American Nat'l Bank of Cheyenne, 401 F.2d 458 (10th Cir. 1968); Gibson v. Alaska Alcoholic Beverage Control Bd., 377 F. Supp. 151 (D. Alaska 1974). *But cf. In re* Midland Services, Inc., 10 U.C.C. Rep. Serv. (Callaghan) 499 (D. Neb. 1971).

11. *See* Semple, *The Legal Incidence of Computer Software in its Use as Collateral in Secured Transactions*, 7 CANADIAN BUS. L. J. 450 (1982-83).

12. *Id.* at 455.

13. *See* discussion *infra* at § IV.

14. *See* Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3d Cir. 1983); Williams Elecs., Inc. v. Arctic Int'l, Inc., 685 F.2d 870 (3d Cir. 1982); Hubco Data Prods. Corp. v. Management Assistance, Inc., COPYRIGHT L. REP. (CCH) ¶ 25,529 (D. Idaho 1983); Apple Computer, Inc. v. Formula Int'l, Inc., 562 F. Supp. 775 (C. D. Cal. 1983); Tandy Corp. v. Personal Micro Computers, Inc., 524 F. Supp. 171 (N.D. Cal. 1981).

15. 17 U.S.C. § 301 (1982).

that apply to a security interest. Clearly, the Copyright Act preempts the Article Nine filing provisions with regard to assignments of copyright,[16] but it does not seem to contain sufficient provisions regulating the rights of the parties and third parties to exclude security interests in copyrights from the provisions of Article Nine. The exclusionary language in U.C.C. section 9-104(a) applies only "to the extent that [the federal copyright law] governs the rights of the parties . . . ." Therefore, if the federal copyright law contains no provisions governing the rights of the parties (concerning security interests and software locks), it might not preempt Article Nine.[17] The federal copyright law preemption issue seems to be less of an impediment to the establishment of an Article Nine security interest in the case of a software lock attaching to a mere license to use the software, as opposed to a transfer of ownership of the copyright in the software.

Assuming that the GENDOC License Agreement is a "security agreement" and the software lock in the GENDOC is a valid security interest, what are the rights and obligations of the parties? Without regard to Article Nine, the terms of the License Agreement govern. If the licensee fails to make a payment when due, and still fails to make the payment after the appropriate cure period and notice, the agreement terminates by its own terms and the licensee has agreed that the software may be made inoperable.

What additional rights and obligations are imposed by placing the transaction under Article Nine? First, if the licensor/secured party perfected its security interest, then the rights of the licensor/secured party extend to third parties. For instance, if the licensee/debtor executes an assignment for the benefit of creditors, the licensor/secured party's rights would extend to the assignee. Presumably, the same would be true with regard to a trustee in bankruptcy.

Part 5 of Article Nine sets forth the rights, remedies and duties of a secured party upon default. U.C.C. section 9-501(1) provides that a secured party has the rights set forth in Part 5, as well as the rights set forth in the security agreement, except as those rights may be limited by section 9-501(3). Section 9-501(3) generally requires the secured party to act in a commercially reasonable manner in disposing of or otherwise acting with regard to the collateral.

---

16. *See* 17 U.S.C. § 205 (1982).

17. U.C.C. § 9-104 comment 1 (1981). *See* CLARK, THE LAW OF SECURED TRANSACTIONS UNDER THE UNIFORM COMMERCIAL CODE ¶ 1.8[1][e] (1980); Bank of Hendersonville v. Red Baron Flying Club, Inc., 571 S.W.2d 152 (Tenn. Ct. App. 1977), cert. denied, 439 U.S. 1089 (1978). *But cf.* Dowell v. Beach Acceptance Corp., 3 Cal. 3d 544, 476 P.2d 401, 91 Cal. Rptr. 1 (1970), *cert. denied*, 404 U.S. 823 (1971).

U.C.C. section 9-503 deals with self-help repossession, which is essentially what a software lock is designed to accomplish. That section allows a secured party to repossess the collateral without judicial process if this can be done without breach of the peace. As an alternative to removal of the collateral, a secured party may render "equipment" unusable. A software lock is a device to render the collateral unusable, but the difficult question is whether the collateral in this case can be considered "equipment." This is where the technical distinction between "goods" and "general intangibles" with regard to software may become relevant. If software is considered to be a "good," it is "equipment,"[18] and may be disabled under section 9-503.

If software is not "goods," is the "render unusable" provision of section 9-503 inapplicable? Perhaps so, but it is arguable that insistence on a strict reading of the word "equipment" in section 9-503 is inconsistent with the intent of the drafters and the stated purpose of the Uniform Commercial Code that it "shall be liberally construed and applied to promote its underlying purposes and policies."[19]

IV. THE SOFTWARE LOCK AS A VEHICLE FOR TORTIOUS OR OTHER WRONGFUL ACTS

A software vendor must exercise considerable care when using a software lock. A direct relationship probably exists between the degree of sophistication of the device and the chance that it will contain a bug that will incorrectly trip the lock. The vendor must balance its own interest in security against the right of its customers to be free from unreasonable risks of harm. For example, a vendor of software designed to monitor the vital processes of patients in a hospital intensive care unit would be foolhardy to employ any type of software lock. On the other hand, the use of a fully tested software lock in a demonstration version of a nonvital piece of software is a safe and prudent course of action for that vendor, since the risk of harm if such a software lock is accidentally tripped is minimal. Traditional tort law principles adequately govern the balance between the vendor's security and the user's risk of harm. In an appropriate case, the imposition of exemplary damages for the unreasonable and perhaps outrageous use of a software lock would be appropriate.

As a supplement to traditional tort law, many states have

18. U.C.C. § 9-109 categorizes goods into four classes: consumer goods, equipment, farm products and inventory. Goods are "equipment" if they are not included in the definitions of inventory, farm products or consumer goods.

19. U.C.C. § 1-102 (1981).

adopted consumer protection laws, often referred to as "Baby FTC" statutes.[20] Many of these statutes apply to businesses as well as to individual consumers. While the author has been unable to find any reported case dealing with the issue of whether a software lock constitutes an "unfair and deceptive" practice, it is not difficult to imagine a set of facts that might state a claim under an unfair trade practice statute.

For instance, suppose a software vendor includes a software lock in a non-demonstration version of payroll software used by a business, and does not disclose to the user the existence of the lock. The agreement between the vendor and user requires the user to make periodic payments. For one reason or another, a payment is not made. The software lock then trips, disabling the software without any notice to the user. As a result, the user is unable to meet its payroll obligations, incurring legal liability to its employees and suffering damages in the form of labor unrest. The user sues the vendor, with the gravaman of the complaint being that the undisclosed software lock and its activation without notice constitutes an unfair or deceptive act or practice. It is likely that the vendor's motion to dismiss such a claim for failure to state grounds for relief would be denied.

On the other hand, if the facts stated above were varied so that the agreement between the vendor and the user was substantially similar to the agreement provided in the Appendix, the motion to dismiss might be more compelling. First, Paragraph 7 of the Agreement discloses the existence of the software lock to the user. Furthermore, assuming the vendor gave the user notice of default as specified in the Agreement, activation of the software lock would be accomplished only after the user received notice and an opportunity to cure.

In one case,[21] the Massachusetts Supreme Judicial Court held that repossession without notice under a security agreement and U.C.C. section 9-503 was not unconscionable, nor was it a violation of Massachusetts General Laws chapter 93A (unfair or deceptive acts or practices). "If Penney was surprised by the repossession, he was not surprised unfairly."[22]

The standard of what constitutes unfair and deceptive acts or

20. *See, e.g.*, MASS. GEN. LAWS ANN. ch. 93A (West 1984); Consumer Fraud and Deceptive Trade Practices Act, §§ 1,2; ILL. REV. STAT. ch. 121½ §§ 261-272 (1983); Unif. Deceptive Trade Practices Act, § 1, ILL. REV. STAT. ch. 121½, §§ 311-317 (1965).

Similar statutes have been enacted in at least 22 jurisdictions. *See* Benedetto, *The Illinois Consumer Protection Act*, 69 ILL. B. J. 350 (Feb. 1981).

21. Penney v. First Nat'l Bank of Boston, 385 Mass. 715, 433 N.E.2d 901 (1982).

22. *Id.* at 722, 433 N.E.2d at 906.

practices ought to be the same whether the issue is the activation of a software lock or the repossession without notice of a fishing boat pledged as collateral for a bank loan. In either case, the standard ought to be one of commercial reasonableness. The harm that could befall the victim in either case must be measured against the legitimate security needs and commercial reasonableness of the actions of the lender or software vendor. One statement of the governing standard in a commercial context was provided by Judge Kass of the Massachusetts Appeals Court: "The objectionable conduct must attain a level of rascality that would raise on eyebrow of one inured to the rough and tumble of the world of commerce."[23] Of course, software is now being licensed to users for personal, household and family purposes. The standard in this context is certain to be balanced more heavily in favor of the consumer-user.

Article Nine itself imposes substantial duties on the secured party to act in a commercially reasonable manner. Sanctions exist under Part 5 of Article Nine for creditor misbehavior. Many of the provisions under Part 5 deal with the creditor's obligations on disposition of the collateral after it is repossessed. Those requirements appear to be inapplicable to the activation of a software lock, since the software is not going to be resold by the creditor, but only disabled in the hands of the debtor. However, the creditor must be careful to avoid violating these requirements when repossessing or deactivating software.

One interesting question is whether the activation of a software lock might involve a breach of the peace. Typically, cases discussing the issue of self-help repossession involving possible breaches of the peace deal with situations where there was an actual or threatened physical confrontation directly related to the repossession. The typical case involves the repossession of an automobile from the debtor's driveway and involves the threat of physical or constructive harm by threats or intimidation. If the threatened harm is not physical, there is no breach of the peace.[24]

Wrongful repossession, however, will subject the secured party to liability.[25] There is a line of cases involving wrongful reposses-

23. Levings v. Forbes and Wallace, Inc., 8 Mass. App. Ct. 498, 504, 396 N.E.2d 149, 153 (1979). *But see* Hanner v. Classic Auto Body, 10 Mass. App. Ct. 121, 406 N.E.2d 686 (1980) (repairman's unauthorized towing of car in attempt to collect repair amounted to unfair or deceptive practice).

24. Thompson v. Ford Motor Credit Co., 550 F.2d 256 (5th Cir. 1977) (conniving and lying in the absence of actual or constructive force used to repossess defaulted debtor's auto did not amount to a breach of the peace).

25. *See, e.g.*, Warren v. Ford Motor Credit Co., 693 F.2d 1373 (11th Cir. 1982) (repossession of automobile without notice held to be a conversion).

sions triggered by inaccurate computer data. In some cases, punitive damages were awarded to the victims as a warning to creditors who rely too heavily on computers to make these decisions.[26] Software vendors who use software locks would be wise to heed the teachings of those cases, especially when the users are individual consumers.

CONCLUSION

It is apparent that there is a great need for software locks or other security devices to prevent or minimize the unauthorized use of computer software. In light of this fact, the software lock, coupled with a license agreement such as provided in the Appendix, ought to be enforceable under traditional contract law. Although it is currently unclear, the software lock might also be enforceable as a "security interest" under U.C.C. Article Nine.

While the software lock's misuse can work a substantial hardship upon users, the vendor's potential liability under traditional tort principles, consumer protection statutes proscribing unfair and deceptive practices, and the sanctions for creditor misbehavior under U.C.C. Article Nine, Part 5 ought to limit such misuse. The failure to disclose the existence of a lock is a prime candidate for the imposition of such liability.

It is likely that the first widely reported cases involving software locks will in large part determine their future use, and the legal posture in which such cases arise will be significant. If the issue involves the enforceability of a software lock agreement under U.C.C. Article Nine, the lock may be found to be an acceptable, albeit modern, form of security interest. If, on the other hand, these first cases involve charges of careless use, improper activation, or wrongful "repossession," the resulting publicity might inhibit their future use.

APPENDIX A

LICENSE AGREEMENT FOR GENDOC SOFTWARE

1. *Parties.* Agreement made this ___ day of _____, 198_ by and between ABC, Inc., a Massachusetts corporation having a place of business at 456 Lotus Street, Revere, Massachusetts 00000 (hereinafter referred to as "Licensee"), and XYZ Corporation, 112 Star

26. Ford Motor Credit Co. v. Hitchcock, 116 Ga. App. 563, 158 S.E.2d 468 (1967) ($5,000 punitive damages awarded); Swarens v. Ford Motor Credit Co., 447 S.W.2d 53 (Ct. App. Ky. 1969) ($5,000 punitive damages awarded); Price v. Ford Motor Credit Co., 530 S.W.2d 249 (Ct. App. Mo. 1975) ($25,000 punitive damages awarded). *See also* Palmer v. Columbia Gas of Ohio, Inc., 479 F.2d 153 (6th Cir. 1973) (class action for improper gas company shutoffs via computer; due process violation).

Road, Boston, Massachusetts 11111 (hereinafter referred to as "Owner").

2. *Grant of License.* Owner hereby grants Licensee a non-exclusive and non-transferable License to use the computer programs jointly known as the GENDOC. On or about February 1, 198—, Owner shall deliver to Licensee a working copy of the GENDOC for use on Licensee's IBM System/38. Licensee is specifically not granted any right to market any version of the GENDOC.

3. *License Fee.* The license fee for the use of the GENDOC by Licensee is $150 per month, payable quarterly in advance. Owner agrees to provide up to three hours of support service per month at no additional charge. Licensee agrees to pay, within fifteen days of invoice, Owner's then current standard hourly charge for all support services rendered by Owner in excess of three hours per month. Owner's now current standard hourly charge is $60 per hour.

4. *Enhancements to GENDOC.* Licensee may ask Owner to make improvements to the GENDOC. Should the requested improvements be recognized as enhancing the marketability of the GENDOC, Owner may agree to make such improvements for no additional charge. If, in the opinion of Owner, the improvements would not make the GENDOC more suitable to the general marketplace, but specifically to the benefit of Licensee, such improvements may be made at Owner's discretion and at Owner's then current standard hourly charge, which shall be paid within fifteen days of invoice.

5. *Restrictions on Use.* Licensee acknowledges that the GENDOC is a valuable trade secret of Owner. Licensee warrants that it has no source code versions of the GENDOC in its possession or control. Owner authorizes Licensee to use the GENDOC only on the single computer system at Licensee's site. Licensee may not disclose, sell, assign, give, allow access to or use of, or otherwise transfer this License or the GENDOC to any third person without Owner's prior written approval. Licensee shall safeguard any and all copies of the GENDOC against unauthorized disclosure and take such steps as are necessary to insure that the provisions of this Agreement are not violated by anyone in the service of Licensee. Licensee shall not disassemble, reverse-compile or tamper in any way with the GENDOC.

6. *Disclaimer of Warranty and Limitation of Liability.* This license to use the GENDOC is granted "AS IS." OWNER MAKES NO WARRANTIES EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE GENDOC. THERE IS NO WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PUR-

POSE. THE ENTIRE RISK AS TO THE GENDOC'S QUALITY AND PERFORMANCE IS WITH LICENSEE. IN NO EVENT SHALL OWNER BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE GENDOC OR THE SUPPORT SERVICES RENDERED BY OWNER HEREUNDER.

7. *Termination of License.* The License granted hereunder shall terminate immediately and the GENDOC programs shall be rendered inoperable without further notice by Owner upon the occurrence of any of the following:

a. Any default by Licensee of this Agreement which is not cured within thirty (30) days after written notice thereof by Owner.

b. The default by Licensee, which is not cured within sixty (60) days after written notice from Owner, of the Software Distribution Agreement between Owner and Licensee dated April 1, 198—, as it may be amended hereafter.

c. Any payment due Owner pursuant to any agreement between Licensee and any Owner which is not paid within fifteen (15) days of the date when such payment is due.

d. Ninety (90) days from written notice from Licensee to Owner seeking to terminate this Agreement accompanied by a written certification by Licensee that the GENDOC and all copies of any version thereof in Licensee's possession or control have been returned to Owner.

e. The failure or refusal of Licensee, after reasonable notice, to allow Owner access to the computer on which the GENDOC is operating for the purpose of reinitializing or resetting the automatic shut-down feature of the GENDOC.

8. *Marketing of GENDOC.* Licensee hereby acknowledges that it has elected to use for its own business purposes, but not to distribute or market the GENDOC programs which are the subject of this Agreement. If Licensee elects to market a GENDOC or like program which it obtains from a source other than Owner, hereafter "Alternate Program," Licensee agrees that:

a. Licensee shall give Owner at least ninety (90) days prior written notice of its intent to so market or distribute said Alternate Program; and

b. Owner or Owner's designated representative shall have the right to examine the Alternate Program for the purpose of determining if said Alternate Program infringes any right of Owner in the GENDOC programs.

9. *General Terms.* This Agreement states the entire agreement between the parties. No amendment or modification of this Agreement shall be made except by an instrument in writing signed by

both parties. This Agreement may not be assigned, in whole or in part, by either party without consent of the other, which consent shall not be unreasonably withheld, except that Owner may assign its interest in all or part of the payments due it hereunder upon notice in writing to Licensee. This Agreement shall be governed and interpreted in accordance with the laws of the Commonwealth of Massachusetts. If any provision of this Agreement shall be held to be unenforceable, such holding shall not affect the enforceability of any other provision hereof. The obligations of Licensee under Paragraphs 5 and 8 shall survive the termination of this Agreement.

By: _____
President
ABC Corporation

By: _____
President
XYZ Corporation