

NEWS



BUSINESS LAW

LETTER

MSBA SECTION OF BUSINESS LAW

Vol. Nine No. Two
Fall 2005

<http://www.msba.org>

Corporate Uncertainty in Records Management: What's Audio Got to Do with It?

*By Elizabeth Kidd, Esq.
Legal Consultant, iCite Legal,
a division of Aspen Systems Corporation*

Corporations are facing a great deal of uncertainty when it comes to managing records in the context of litigation and regulatory investigations. Take the case of Rambus, Inc., a memory chip designer that was penalized for destruction of emails. In *Rambus, Inc. v. Infineon Tech. AG*, 220 F.R.D. 264 (E.D. Va. 2004), the court sanctioned the Company for spoliation of evidence even though there was no litigation planned, no clear duty to preserve the records in question, and no showing of prejudice or bad faith.

To add to the uncertainty, standards and guidelines for corporate compliance are decidedly lacking under the myriad of new rules and regulations. This is especially true for companies in heavily regulated industries, such as the financial and energy markets. The legal landscape gets even cloudier when it comes to audio records such as voice mails, phone call logging databases for brokerage houses and customer call centers, Voice over Internet Protocol (VoIP), Unified Messaging Systems (UMS), and other audio records.

What do audio records have to do with electronic discovery? Apparently, a lot. The Commodities Futures Trading Commission (CFTC) fined Duke Energy \$28,000,000 when it discovered that Duke traders submitted false market information using telephones, faxes, and emails. See *In the Matter of Duke Energy Trading and Marketing, L.L.C.* before the CFTC, Docket No. 03-26, September 17, 2003; [CFTC Press Release 4840-03](#). The CFTC recently launched multiple federal actions against energy traders charging them with false reporting and attempted market manipulation. Audio evidence is featured in at least two of those actions. See *CFTC v. Bradley, and Martin*; and *CFTC v. Atha, McDonald and Whalen* at [CFTC Press Release 5045-05](#).

Corporate counsel recently had the opportunity to outline some of the daunting challenges facing corporations

today. Public hearings were held in February, 2005, before the Advisory Committee on the proposed amendments to the Federal Rules of Civil Procedure regarding electronic discovery. In his testimony on behalf of the Association of Corporate Counsel (ACC), Lawrence La Sala explained to the Committee that "electronic discovery and records retention challenges often top the list of concerns faced by [members of the ACC] and their clients...the issue affects and frustrates organizations of every size, shape and color." <http://www.uscourts.gov/rules/e-discovery/CVHearingFeb2005.pdf> at p. 362.

Corporate America has expended considerable resources in the last couple of years just to ensure that their records management and reporting policies comply with

(continued on page 5)

Table of Contents

- *Corporate Uncertainty in Records Management: What's Audio Got to Do with It?* 1
- *Precaution to Be Taken Against Identity Theft* 2
- *Software Piracy: Tips on How to Avoid Breaking the Law* 3
- *Corporate Legislative Update* 4

Precaution to Be Taken Against Identity Theft

By John H. Denick, Esq.
Baltimore, Maryland

Identity theft is a growing problem. Fortunately, there are some simple steps that you can take to protect yourself and your credit. Please feel free to share this information with your family, friends, co-workers, and employees.

CHECKS

When ordering checks, only have your first initial (instead of the full name) and last name printed on them. This way, someone who takes your checks will not know your first name and thus will have trouble forging your signature. Secondly, have your work phone number printed on your checks instead of your home number, and use either a P.O. Box address or your work address (where practical) instead of your home address to minimize the amount of personal information a thief can obtain from your checks. Avoid placing other personal information such as your driver's license number on your checks. Finally, **NEVER** have your Social Security number printed on checks; this is possibly the single most dangerous piece of information for a thief to have.

WALLET

Make photocopies of every item in your wallet, both front and back, so that you will have all your account numbers, important phone numbers, and other pertinent information on hand if your wallet is stolen. This will also serve as an inventory so that you will know exactly what information the thief now has. Keep this information in a safe but handy place in the event you should need it.

CREDIT CARDS

When paying your credit card bill by check, only write the last four digits of your account number in the memo line, not the full account number as credit card companies request. This way, those processing your check will not have access to the full number. The last four digits are the

only ones necessary for the credit card company to identify you. Further, be sure to keep a copy of your card numbers and a list of the toll free numbers necessary to cancel your credit cards should they be stolen.

If they are stolen, the following simple steps can greatly reduce the damage done to your credit. Take them **IMMEDIATELY** for your own protection.

1) File a police report in the jurisdiction where your wallet was stolen. This serves as notice to credit providers of your diligence and is a first step toward an investigation.

2) Call the three national credit reporting organizations and the Social Security Administration Fraud Line to place a fraud alert on your name and Social Security number. This way, any company that checks your credit will know that your information was stolen and will contact you by phone to authorize new credit.

The numbers are:

Equifax: 1-800-525-6285

Experian (formerly TRW): 1-888-397-3742

Trans Union: 1-800-680-7289

Social Security Administration Fraud

Line: 1-800-269-0271

Calling these numbers should be the first step you take if your wallet is stolen.

MAIL, RECEIPTS, AND OTHER DOCUMENTS

If possible, invest in a shredder. Shred solicitations for credit cards and mortgage applications so that if a thief goes through your trash, the application form cannot be retrieved. Other documents containing identifying information, such as credit card statements, receipts, certain medical and business statements, and tax return information should also be shredded prior to disposal.

Following these simple steps will greatly minimize the damage a thief can do by stealing your checks, credit cards or other identifying information from other documents.



Software Piracy: Tips on How to Avoid Breaking the Law

*By Frank Morgan, Esq.
Hodes, Ulman, Pessin & Katz, P.A.*

The Intellectual Property Committee of the Business Section met on February 9, 2005, to hear a presentation by Philadelphia attorney, M. Kelly Tillery, Esq., of Leonard, Tillery & Sciolla, LLP, on the activities of his client, the Business Software Alliance (“BSA”), and other software company trade associations in enforcing the copyright laws against software piracy.

When a business “buys” software, what is really happening in almost every case is that the business is purchasing a license to use the software. Ownership of the software remains with the company that created it. Software is the intellectual property of its owner and cannot be reproduced, distributed or used except according to the terms of the license which accompanies authorized copies of the software.

Software piracy refers to the illegal use of software. For example, installing on company computers software that was purchased at a “too good to be true” price at a weekend flea market violates the copyright of the software’s creator if the “bargain” software is an unauthorized copy of the original. Even if software

is acquired under a legitimate license, software piracy can occur if the terms of the license are violated; for example, by installing the same copy of a single-user program on several computers.

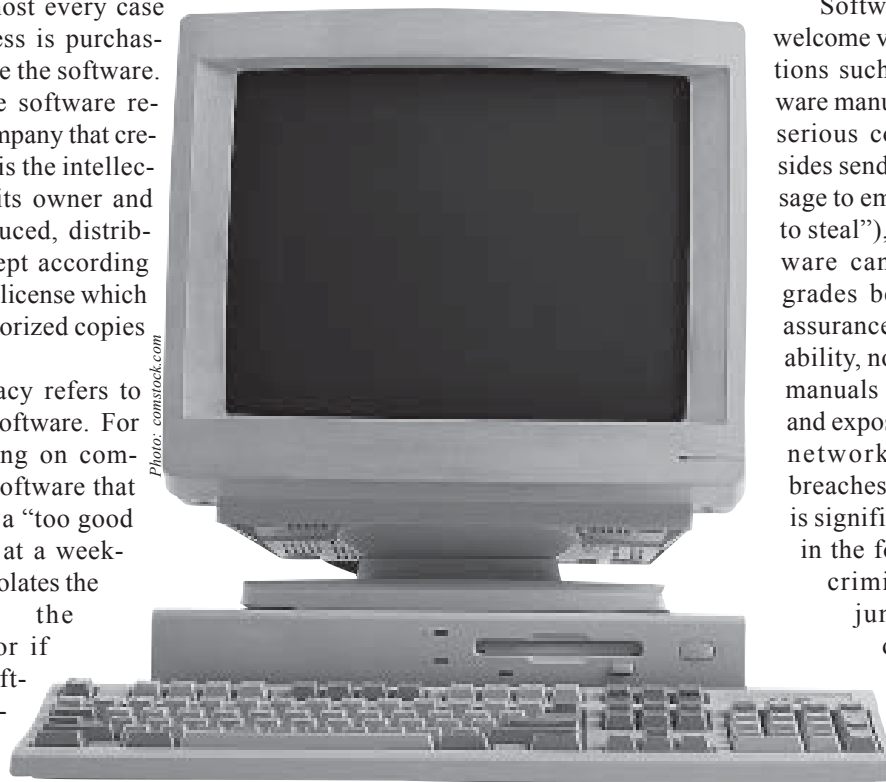
The Business Software Alliance (BSA) is one of several software trade associations whose goal is to enforce the copyright laws against businesses suspected of software piracy. In a typical scenario, an employee with a grudge will contact BSA and report that his former employer has made unauthorized copies and/or installed unlicensed software owned by one of BSA’s members. Attorneys for BSA will contact the accused business

owner and request that he or she produce all software licenses and purchase documentation. If the company is unable to show that its software is properly licensed, BSA will demand that all illegal software be removed, require that the company enter into proper licenses, and seek compensation for unauthorized use as well as payment for BSA’s expenses and attorneys’ fees incurred in enforcing the law.

Software piracy, and unwelcome visits from organizations such as BSA and software manufacturers, can have serious consequences. Besides sending the wrong message to employees (“It’s okay to steal”), using pirated software can result in no upgrades being available, no assurance of quality or reliability, no technical support, manuals or documentation, and exposure of a company’s network to security breaches. In addition, there is significant legal exposure in the form of civil and/or criminal penalties, injunctions, monetary damages, and attorneys’ fees and costs.

The risk of being charged with software pi-

racity can be reduced significantly by taking proactive measures to manage software assets. A company should have a stated policy of intolerance for software piracy. There should be procedures in place for acquiring and documenting the purchase of only legitimate licensed software and rules that prohibit employees from downloading software from the Internet. Software should not be installed on more computers than authorized by the software license. Regular self-audits of software usage and periodic examination of license and purchase documents can reduce the risk of unauthorized software being used on company computers.



Corporate Legislative Update

By Whiteford, Taylor & Preston L.L.P.
7 Saint Paul Street
Baltimore, Maryland 21202
www.wtplaw.com

Listed below are several bills of general interest to corporate attorneys. This list only highlights certain bills before and/or passed by the Maryland legislature, and is not meant to include a full list or discussion of each and every bill.

1. **Labor and Employment - Minimum Wage – Increase (HB 391) (1/01/06)**. HB 391 was passed by the legislature but was vetoed by Governor Ehrlich on May 20, 2005. The Bill would have raised the minimum wage in Maryland to the greater of the federal rate (currently \$5.15 per hour) or the new state-set rate of \$6.15 per hour.

2. **Corporations and Real Estate Investment Trusts – Miscellaneous Provisions (HB 958) (6/01/05)**. This Bill, among other things, expands the costs directors of a corporation may obtain from the corporation after successfully defending himself or herself. Although prior law permitted statutory recovery only for the successful defense of proceedings, the new law includes costs incurred in the successful defense of claims, issues, and matters as well.

3. **Film Production Activity - Employer Wage Rebate Grant Program (HB 253/SB 215) (7/01/05)**. These Bills establish programs within the Department of Business and Economic Development to provide qualified film producers engaging in film production activity in the State a rebate of fifty percent (50%) of the first \$25,000 of each qualified employee's wages, up to a maximum of \$2,000,000 for each production. The rebate does not apply to employees earning over \$1 million for a production. To qualify for the rebate, a film production activity must be intended for nationwide distribution and have direct costs in the State of at least \$500,000. The fiscal 2006 budget includes \$4,000,000 for this new program. The Bills include specific reporting requirements to assist in evaluating how well the program works in stimulating local employment in film.

4. **Commercial Law – Gift Certificates and Gift Cards – Expiration and Fees – Restrictions (SB 8) (7/01/06)**. After several years, and the passage of similar laws in various other states, Maryland has adopted restrictions and prohibitions on the expiration and service fees relating to gift certificates and gift cards. The Bill prohibits the expiration of, or imposition of a fee on, any gift certificate or gift card within four (4) years of the date of purchase. In the event the gift certificate or gift card expires or a fee is assessed on the card after the four (4)-year period, certain

terms must be displayed in at least ten point font on the certificate or card.

5. **Financial Regulation – Debt Management Services (HB 753) (10/01/05)**. In response to consumer complaints about debt adjustment services, the General Assembly passed the Maryland Debt Management Services Act in 2003. The Act established licensing requirements and other measures to regulate the debt management services industry. This Bill expands regulatory oversight over debt management services providers by: (1) prohibiting insider dealing, false advertising, and sales incentives to employees for enrolling consumers in debt management plans or agreements; (2) increasing the maximum amount of the bond a debt management services provider must post from \$350,000 to \$1,000,000; and (3) increasing the disclosures an applicant must make to receive a license. The Bill also implements a sliding scale fee schedule based on annual gross revenue for initial and renewal licenses and clarifies that the Maryland Debt Management Services Act applies whether or not the debt management services provider has an office in Maryland. Finally, the Bill requires the Commissioner of Financial Regulation and the Attorney General jointly to: (1) study the impact of the Bill on consumers and debt management services providers, regulatory mechanisms used in other parts of the country, and the impact of authorizing for-profit entities to provide debt management services in the State; (2) recommend any appropriate changes to the Maryland Debt Management Services Act; and (3) report their findings and recommendations to the House Economic Matters Committee and the Senate Finance Committee by December 31, 2006.

6. **Consumer Protection – Privacy of Social Security Numbers (HB 56) (1/01/06)**. This Bill prohibits a person, except a unit of State or local government, from: (1) publicly posting or displaying an individual's Social Security number ("SSN"); (2) printing an individual's SSN on a card required for the individual to access products or services provided by the person; (3) requiring an individual to transmit the individual's SSN over the Internet unless the connection is secure or the individual's SSN is encrypted; (4) initiating the transmission of an individual's SSN over the Internet unless the connection is secure or the individual's SSN is encrypted; or (5) requiring an individual to use the individual's SSN to access

(continued on page 5)

Records . . .

(continued from page 1)

the Sarbanes Oxley Act of 2002. But companies are finding that becoming “SOX compliant” is not enough. New record retention laws have impacted virtually every industry. What’s more, regulatory audits and investigations are on the rise. At a recent energy conference in Washington, D.C., the Deputy Director of an enforcement arm of the Federal Energy Regulatory Commission (FERC) said that there has been a ten-fold increase in the number of investigations and audits since Enron. The CFTC alone has levied close to \$300 million in civil penalties since the fall of Enron. Add to the mix the spate of civil law suits frequently filed on the heels of many regulatory actions, and what you find are corporations struggling to keep up with the management, review, and production of enormous volumes of records.

In light of a few high profile cases of corporate fraud, no company wants to be the first to suggest that regulatory document demands are unreasonable, overly broad or burdensome. As a result, companies are frequently bending over backwards to comply with sometimes sweeping demands for everything from paper files, to emails, voice mails, instant messages, compressed digital information captured on back up tapes, and calls logged into databases by traders or customer call centers. The costs associated with restoring back up tapes, searching for relevant records, reviewing them for privilege and proprietary information, and then producing them are often enormous. Though most companies are making good faith efforts to comply, in a word, corporations are tired. And they are spending a great deal of time and money on activities that have little or nothing to do with running the business.

Unlike in litigation, corporations usually have only thirty days to produce records demanded in a regulatory investigation. Often there is no time to review the massive collections of audio records stored in company servers. Some corporate counsel have suggested that voice mails do not fall squarely within the definition of a “document” under the Federal Rules of Civil Procedure or under the plethora of new rules and regulations pertaining to document retention requirements.

There is some merit to that argument. While many of the new rules specifically mention emails, they are frequently silent on the disposition of voice mails and other audio records. The regulators themselves admit that they do not have clearly defined standards and guidelines outlining what penalties apply to which document retention violations. But one thing is clear. Judges and enforcement officers of regulatory agencies such as the FERC and CFTC do indeed view voice mails as “documents” subject to their audit and investigative demands. The same is true of Instant Messages, VoIP, UMS, call logging databases and other audio records. When a damning phone call is discovered, it is

virtually impossible to defend against. According to Mr. Pease, one investigation settled – to the tune of \$14 million – immediately after the FERC found audio evidence of a trader making an illegal trade.

The news is not all bad. For the most part, regulatory agencies are working with companies trying to bring them into compliance rather than pursuing an agenda to punish. Corporations that come to regulatory bodies when they’ve discovered a problem stand in a much better position than those who are found with violations in an investigation or audit. In addition, there are a number of actions companies can take to mitigate the risks of sanctions and set up safe guards to help them navigate through the current uncertainty, including:

(continued on page 6)

Update . . .

(continued from page 4)

an Internet web site unless a password, unique personal identification number, or other authentication device also is required to access the web site.

Similarly, unless required by State or federal law, the Bill prohibits such a person from: (1) printing an individual’s SSN on material mailed to the individual; (2) including an individual’s SSN in material that is electronically transmitted to the individual unless the connection is secure or the individual’s SSN is encrypted; or (3) including an individual’s SSN in any material that is transmitted by facsimile to the individual. The prohibitions listed above do not apply to: (1) the collection, release, or use of an SSN as required by State or federal law; (2) the inclusion of an SSN in an application, form, or document sent by mail, electronically transmitted, or transmitted by facsimile under specified circumstances; (3) the use of an SSN for internal verification or administrative purposes; or (4) an interactive computer service provider’s or telecommunications provider’s transmission or routing or temporary storage of an SSN.

A person that used an individual’s SSN before January 1, 2006, in a manner prohibited by the Bill may continue to do so until January 1, 2009, if: (1) the use is continuous; and (2) the person provides an annual disclosure form stating the individual’s right to stop the use of the individual’s SSN. A request to stop using an individual’s SSN must be implemented within 30 days after receipt. Furthermore, a person may not deny products or services to an individual because of a request to stop using the individual’s SSN.

Records . . .

(continued from page 1)

1. Develop a comprehensive records management plan that addresses not only the company's day-to-day operational needs and obligations in terms of regulatory compliance, but also with an eye to risk management in responding quickly and efficiently to investigations, audits, and lawsuits;

2. Include the IT department, in-house counsel, and at least one high level officer on the company's records management team, especially if it's still in the planning stages;

3. Conduct regular due diligence on corporate records management policies and procedures and set a schedule to update them regularly;

4. Develop policies and procedures designed specifically to respond to litigation holds, document requests, and investigative audits, and make sure they are communicated to employees;

5. Ensure that compliance officers have true independence in the corporate reporting structure and give them unfettered access to employees and officers throughout the company;

6. Set up and maintain on-going employee training in records management;

7. Compliance officers should review and update employee training procedures;

8. Regularly update corporate organization charts, job titles, and job descriptions;

9. Establish a hot line for employees to anonymously report issues as they arise and document the responsive actions taken;

10. Conduct periodic reviews and audits, either inter-

nally or with an outside firm;

11. Document the findings as well as the steps taken to correct problems;

12. Maintain audit reports with the supporting documentation and be able to produce them quickly and efficiently.

There is no denying the uncertainty in the legal framework surrounding record management today, particularly when it comes to audio records. Given the trend towards greater sanctions, increased investigations, and the introduction of random audits, corporations have legitimate concerns. The key is documentation, a well thought-out and executed records management plan, regular audits, and remediation as needed. The greater a company's ability to show courts and investigators that they are doing all they can to come into compliance with all the new rules and regulations (even when the rules are vague), the better off they will fare when it comes to avoiding or mitigating sanctions and civil penalties. Likewise, the more efficiently corporations can respond to document requests, the better their position to defend against allegations of willfully destroying evidence, or even inadvertently deleting records. Developing an enterprise records management plan, which includes audio records, may cost a little more on the front end, but at the end of the day, it can go a long way to reducing a company's overall costs and risks associated with a piecemeal records management approach.

© 2005 Elizabeth Kidd – All rights reserved; permission to use granted to MSBA Section of Business Law.

SECTION OF BUSINESS LAW NEWSLETTER

Maryland State Bar Association

Submissions, questions, comments?

EDITOR:

Joseph P. Ward, Esquire
 Whiteford, Taylor & Preston L.L.P.
 7 Saint Paul Street, Suite 1400
 Baltimore, Maryland 21202
 (410) 659-6432
 fax (410) 347-9414
 jward@wtplaw.com

