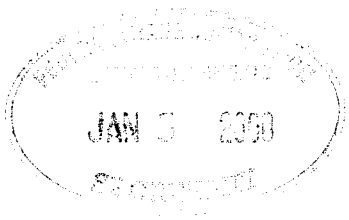
GREENBERG
ATTORNEYS AT LAW
TRAURIG



Spencer G. Feldman
212-801-9221
e-mail: feldmans@gtlaw.com

January 5, 2000

VIA FEDERAL EXPRESS

Mr. David Medine
Associate Director for Financial Practices
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Mr. Medine:

I wish to volunteer for the Advisory Committee On Privacy And Security Online. I am a corporate partner at Greenberg Traurig, a national law firm where I am involved in corporate transactions for Internet companies. My background information is enclosed. I have authored numerous articles on privacy and security issues, copies of several of which are enclosed.

I will be speaking at a seminar titled "Corporate Privacy in the Age of the Internet" later this year and a similar seminar at Albany Law School's Science and Technology Law Center.

Please feel free to contact me if you need more information. I look forward to hearing from you.

Sincerely yours,

Spencer G. Feldman

SGF/dp

Are Your Secrets

Acquisition Confidentiality Agreements in

The pace of mergers and acquisition activity has accelerated. Wheeling and dealing on Internet time has led to a greater willingness of companies to disclose confidential information very quickly in due diligence without appropriate safeguards. The secrets they share in the process of negotiating are often thought to be protected by virtue of the parties entering into an acquisition confidentiality agreement.

As a legal matter, special security measures must be contained in acquisition confidentiality agreements in order to keep pace with advances in Internet and information technology. For the discloser of confidential information, legal considerations and practical protections are available to guard against actions by recipients of such information who might be tempted to defeat the spirit of a confidentiality agreement. At the most basic level, an updated and thorough acquisition confidentiality agreement may deter potential partners from misappropriating confidential information through networked computers and other electronic means.

The widespread use of networked computer systems to store confidential information raises a complex series of issues that all companies must assess. In an acquisition context, it is no longer acceptable for a company to require simply the redelivery or destruction of confidential materials if either party decides not to proceed with a transaction. With computer-based FAX machines, LAN-based personal computers, e-mail and the Internet, image-processing scanners, back-up tape archival procedures and computer "undelete" applications, confidential information can be retained by the recipient without running afoul of the literal terms of many traditional confidentiality agreements. It could then be used to the detriment of the discloser. Without carefully thought-out procedures, such information may be inadvertently retained by the recipient without intent to do so. Following an unsuccessful negotiation, this private data may be uncovered by the next suitor during the due diligence process–who may be a competitor of the original disclosing party.

Safe?

the Internet Age

By Spencer G. Feldman and Constantine S. Potamianos

Strategic Acquisitions

The continuing pace of strategic acquisitions and industry consolidations in the Internet and information technology fields has greatly increased the chance that the recipient of confidential information is a direct competitor. Because many transactions in this field ultimately fail to be completed for a variety of reasons, the potential use of such confidential information by a competitor poses obvious dangers to a company.

In most model forms of acquisition confidentiality agreements, if the transaction is not consummated, the recipient of confidential information is required to return all "written" or "tangible" evaluation materials to the discloser of such information without retaining any copies. By itself, this approach does not take into account the extent of today's Internet and information technology.

FAX Modems and Scanners

One example of the complexity that can arise with the delivery of confidential information in acquisition transactions is when the form of the information is changed. With computer-based FAX modems, confidential information that originates on paper can be stored electronically in the recipient's computer. With the use of image-processing scanners, written materials can also be converted into electronic form and saved indefinitely. Similarly, computer-based audio and video record and playback applications can record confidential information as a permanent record that can be retrieved instantaneously. In each instance, such information is no longer in written form and may arguably not be required to be returned under a literal interpretation of a typical acquisition confidentiality agreement. When it comes to protecting such information, many of the protections indicated for e-mail communications also apply to these electronic communications.

There are ways a company can protect itself from this problem. Because confidential information can be easily changed from its original paper form, the discloser must be assured the recipient will use special security measures to restrict access to confidential information stored on its computer system. For this reason, any computer system containing confidential information should be accessible only by means of password codes and, more importantly, the actual information should be stored in encrypted form. Furthermore, access to the computer system should be compartmentalized.

A separate computer system to receive and store confidential communications with its own dedicated direct modem connection and dedicated Internet identity is the most secure means for containing access to electronic communications. If this is not practical, the following considerations dealing with information in the LAN environment should be considered.

LAN-Based PCs and the Internet

When a discloser's confidential information is stored on a server or a PC connected to the recipient's local area network (LAN), unauthorized personnel can gain entry to the information by accessing files from another computer connected to the LAN. These individuals could then transmit it outside the recipient organization without the knowledge of those involved in the transaction. Similarly, these individuals could copy the files containing confidential information to their notebook, laptop or other mobile computer, which can be physically carried off-site and copied to unsecured PCs.

As the recent controversy at some U.S. nuclear research laboratories indicates, such information deliberately or inadvertently can be transferred from a secure portion of the LAN to a non-secure portion, where it can be accessed by any number of unauthorized persons.

If a company has a connection to the Internet through its LAN, persons external to the company may be able to gain access to computer files on its corporate network if the company does not maintain a firewall. For that matter, even a well-designed firewall may be susceptible to a cleverly executed hacker attack. For this reason, a disclosing company must determine if it is prudent to furnish confidential information before or after a definitive acquisition agreement is executed if the recipient's computer system is a potential security risk. The discloser of confidential information should conduct an audit of the recipient's security procedures and require additional protection against hackers if existing protections are inadequate.

At the very least, confidential information should always be stored and transmitted in an encrypted format. Parties can establish a secure mini-LAN that limits access to

the group of individuals immediately involved in the specific transaction, and tracks and logs specific file access by both individual and access point.

E-Mails and the Internet

Transmission of confidential information by e-mail and e-mail attachment files presents a number of problems. E-mail messages that are embedded in the recipient's e-mail directory must first be labeled appropriately as 'confidential" in all subject fields. Because e-mail can be stored in multiple locations, this will help ensure that sensitive e-mail messages can be identified and deleted if a transaction is not completed.

In order to better maintain the confidentiality of information and safeguard against possible misdirected e-mail and FAX messages, the parties should specifically name a limited group of persons to whom confidential information may be sent, listing their individual e-mail addresses and FAX numbers and whether the FAX is computer-based. This can be easily accomplished in an addendum to the acquisition confidentiality argument. In all e-mail correspondence, the parties should also use a confidentiality banner or disclosure statement (which is now widely used with FAXes) noting that the e-mail is confidential, intended only for the named recipient and may contain information that is legally privileged.

Confidentiality banners are often appended to the end of e-mail messages. Given the nature of e-mail messages and the fact that a recipient must scroll through them to read them, it makes more sense to place such a banner at the very top of the message. If notification features are available through the sender's e-mail system, the sender should request and, upon receipt, store message opening notifications confirming delivery to the appropriate address of e-mail messages (similar to the way in which FAX transmission confirmation sheets are used). The sender also should request that any unintended recipient immediately delete the e-mail message from his or her computer and notify the sender through reply e-mail of the erroneous transmission. This allows the sender to audit the trail of the message and, if system access is granted, delete any system copies.

As a side note, the Federal Trade Commission's Bureau of Competition has also expressed concern that a sham acquisition proposal could be used as a method of exchanging pricing information between competitors in violation of price-fixing laws. It advises companies exploring acquisitions to update confidentiality agreements and determine appropriate limitations regarding who may receive and review confidential and proprietary information.

Back-Up Tapes

Most companies back up data on their computer systems daily, weekly, monthly and/or yearly. If confidential information is saved on a yearly back-up cycle, that information will remain stored on a tape for one year or until the backup tape is recycled or archived. For example, if confidential customer information is received and stored in a computer file on Monday, the system is backed up on Tuesday, a proposed corporate acquisition is terminated on Wednesday and the file is deleted from the computer on Thursday, the Tuesday back-up tape still has the confidential information on it that can be easily restored at any time back onto the computer.

It is impractical, and in some cases impossible, for a company to go back and remove selected confidential information from its archival media. Likewise, it is not feasible to expect a company to redeliver or even destroy its archival back-up tapes, which often contain huge amounts of data, or not to back up its data at all. The best option is for

the company to have a dedicated computer system for the storage of confidential information that is exempt from normal back-up procedures.

Standard confidentiality agreements should be updated to require the recipient to conspicuously place a warning on its back-up tapes that contain confidential information to the effect that if such tapes need to be restored, the discloser of the information shall be notified and the information shall be immediately erased upon its restoration to disk. In addition, as numerous well-publicized litigations have evidenced, e-mail systems that are backed up on a regular basis should never be overlooked in addressing confidentiality concerns in back-up procedures. Likewise, the tapes should be carefully protected through standard physical security restrictions.

File Erasure

Another example of complexity arises when deleted confidential information can be recovered with various software utilities through "undelete" programs. In order to preserve full confidentiality, appropriate files must be erased from the disk or tape itself and not just the link (or pointer) to the files. A number of software programs create temporary working copies of files that sometimes are deleted automatically, but other times remain on the computer system.

Computer systems should be audited on an ongoing basis to remove temporary or working copies of confidential files. Acquisition confidentiality agreements should indicate the file erasure standards to be followed. For example, specific software file utilities are readily available in the commercial marketplace with various levels of deletion security. Some even have military-level deletion capability so the sectors on which a deleted file was stored are overwritten with random data one or more times to ensure that no confidential data can be recovered. As an added security measure, the free space on computer disks that contain confidential files can also be erased, using a utility that overwrites the free space on a disk.

Defining Computer Media

From a legal standpoint, it is arguable whether the term copy includes a computer file in electronic form, or whether it can be considered a copy only when it is printed as a hard copy. This is similar to oral disclosure, which must be reduced to writing in order to be protectable. It is important, therefore, that the scope of confidential information be defined broadly to include information in any format: printed; stored in digital or analog form; electronic and magnetic media; stored images on film or tape; and information stored electronically. Acquisition confidentiality agreements that do not define the information format may be an insufficient form of protection. Recipients can claim they were unaware that specific forms of information or media were considered subject to the prohibitions of confidentiality.

Post-Transaction Security Audit

Given the complex nature of the ways confidential information is exchanged and stored, and the fact that no acquisition confidentiality agreement can anticipate the full range of possibilities, an additional provision for a security audit should be added. In addition to requiring the recipient to return all confidential information, the discloser may demand the right to conduct a security audit following a failed transaction to ensure that all disclosed confidential information on the recipient's computer systems has been erased, returned or adequately protected. As a practical matter, if such a provision is accepted by the recipient at the onset of negotiations, it may also serve to encourage diligent compartmentalization of confidential information by the recipient on an ongoing basis to limit the scope of any post-transaction access to the recipient's systems.

Conclusion

Contractual provision and diligent practical measures can not fully protect a company against the misappropriation of confidential information. Disclosers can safeguard their technology-based confidential information by anticipating the possible problems and building new protections into their standard acquisition confidentiality agreements. It is also important to assess how well the recipient protects its own confidential information. Depending on the nature of the information being provided, such as financial, technical or human resource data, and the industry, added security procedures will be considerably more onerous than necessary. In other instances involving Internet and information technology companies, the procedures may fall short. At the very least, these added security procedures would impress a potential acquisition partner and serve as an indication of both the company's professionalism and how highly it values confidential and proprietary information. ❑

INSIGHTS

THE CORPORATE & SECURITIES LAW ADVISOR

Volume 13, Number 10, November 1999 Aspen Law & Business

Delaware Counsel Marks Up Fiduciary-Out Forms: Part I Page 2

JOHN F. JOHNSTON of Morris, Nichols, Arsht & Tunnel suggests why, especially in light of recent Delaware decisions, the typical fiduciary-out provisions in an acquisition merger agreement should be revised, and solicits responses to a survey on the subject.

Corporate Policies under the Expanded Foreign Corrupt Practices Act Page 10

MICHELLE A. LEWIS of Gibson, Dunn & Crutcher examines the 1998 amendments to the Foreign Corrupt Practices Act and suggests actions companies should take to minimize the risk that their employees, agents, subsidiaries, or consultants will engage in activities that violate the Act.

The Impact of Technology on Acquisition Confidentiality Agreements Page 17

SPENCER G. FELDMAN and **CONSTANTINE S. POTAMIANOS** of Greenberg Traurig discuss the need to revise acquisition confidentiality agreements to reflect the new realities of information exchange, storage, and retrieval.

DEPARTMENTS

MERGERS AND ACQUISITIONS

The Impact of Technology on Acquisition Confidentiality Agreements: Doing Deals in the Internet Age

In the context of mergers and acquisitions, sensitive information is frequently exchanged between the parties to the negotiations, and such disclosures are often protected by means of a standard acquisition confidentiality agreement. As a result of continuing advances in Internet and information technology, a company's standard acquisition confidentiality agreement may be outdated and should be revised to reflect the new realities of information exchange, storage, and retrieval.

by Spencer G. Feldman and Constantine S. Potamianos

The pace of mergers and acquisition activity has accelerated, and the parties to a merger or acquisition must frequently quickly exchange information, engage in negotiations, consummate a transaction, or move on to the next negotiation. Wheeling and dealing on Internet time has led to a greater willingness of companies to disclose confidential information very quickly in due diligence without appropriate safeguards. The secrets they share in the process of negotiating are often thought to be protected by virtue of the parties entering into an acquisition confidentiality agreement. However, as a legal matter, special security measures must be contained in acquisition confidentiality agreements in order to keep pace with advances in Internet and information technology and, as a practical matter, these security measures must be implemented to actually secure the information. For the discloser of confidential information, this article suggests legal considerations and practical protections to guard against actions that may be taken by recipients of such information who might be tempted to defeat the spirit of a confidentiality agreement. At the most basic level, an updated and thorough acquisition confidentiality agreement may deter potential acquisition partners from misappropriating confidential information through networked computers and other electronic means.

The widespread use of networked computer systems to store confidential information raises a complex series of issues that all companies must assess. In an acquisition context, it is no longer acceptable for a company to require simply the redelivery or destruction of confidential materials if either party decides not to proceed with a transaction. With computer-based fax machines, LAN-based personal computers, emails and the Internet, image-processing scanners, backup tape archival procedures, and computer "undelete" applications, confidential information can be retained by the recipient without running afoul of the literal terms of many traditional confidentiality agreements, and then possibly used to the detriment of the discloser of such information. Moreover, without carefully thought-out procedures, such information may be inadvertently retained by the recipient without intent to do so and, following an unsuccessful negotiation, may be uncovered during the due diligence process of the next suitor, who may quite possibly be a competitor of the original disclosing party.

Strategic Acquisitions

The continuing strong pace of strategic acquisitions and industry consolidations in the Internet and information technology fields has greatly increased the chance that the recipient of confidential information is a direct competitor. Because a great many of the transactions in this field ultimately fail to be completed for a variety of reasons (principally among them conflicting corporate cultures and final pricing of the transaction in an environment in which the companies' stock prices are often quite volatile), the potential use of such confidential information by a competitor poses obvious dangers to a company.

In most model forms of acquisition confidentiality agreements, if the transaction is not consummated, the recipient of confidential information is required to re-

Spencer G. Feldman is a partner and Constantine S. Potamianos is an associate at Greenberg Traurig in New York, NY.

turn all "written" or "tangible" evaluation materials to the discloser of such information, without retaining any "copies" thereof. This approach does not, by itself, take into account the extent of today's Internet and information technology.

Fax Modems and Scanners

A good example of the complexity that can arise in connection with the delivery of confidentiality information in acquisition transactions is when the form of the information is changed. With computer-based fax modems, confidential information that originates in paper form can be stored electronically in the recipient's computer when transmitted over open telephone lines or other communications systems and can be subsequently recovered from the recipient's computer. With the use of image-processing scanners, written materials can also be converted into electronic form and saved indefinitely. Similarly, computer-based audio and video record and playback applications can record confidential information as a permanent record and be retrieved instantaneously. In each instance, such information, which is no longer in "written" form and, in most instances, no longer in "tangible" form, may arguably not be required to be returned under a literal interpretation of a typical acquisition confidentiality agreement and, worse, as a practical matter, may not be returnable. With respect to protecting such information, many of the protections indicated for email communications also apply to such other electronic communications.

Because confidential information can be easily changed from its original paper form, the discloser of confidential information must assure itself that the recipient will use special security measures in order to restrict access to confidential information that is stored on its computer system. For this reason, any computer system containing confidential information should be accessible only by means of password codes and, more importantly, the actual information should be stored in encrypted form. Furthermore, access to the computer system should be compartmentalized.

If it is not practical to dedicate a separate computer system to receive and store confidential communications (with, of course, its own dedicated direct modem connection and dedicated Internet identity), which is the most secure means for containing access to electronic communications, then the following considerations dealing with information in the LAN environment should be followed.

LAN-Based PCs and the Internet

When a discloser's confidential information is stored on a server or a PC connected to the recipient's local area network (LAN), unauthorized personnel of the recipient can gain entry to the information by accessing files on one computer from another connected to the LAN. These individuals could then transmit it outside the recipient organization without the knowledge of those involved in the transaction. Similarly, these individuals could copy the files containing confidential information to their notebook, laptop or other mobile computer, which can be physically carried offsite and copied to yet other PCs that may not be secure. As the recent controversy at some of our nuclear research laboratories indicates, such information, deliberately or inadvertently, can be transferred from a secure portion of the LAN to a non-secure portion of the LAN, where it can be accessed by any number of unauthorized persons not cleared to view and download such information.

If a company has a connection to the Internet through its LAN, persons external to the company may be able to gain access to computer files on its corporate network if the company does not maintain a firewall. For that matter, even a well-designed firewall may be susceptible to a cleverly executed hacker attack. For this reason, a disclosing company must determine early on whether to furnish confidential information at a later date after a definitive acquisition agreement is executed or at all if it is believed that the recipient's computer system is a security risk. The discloser of confidential information may well decide to conduct an audit of the recipient's security procedures. A discloser may even require the recipient to obtain added protection against "hackers" if existing protections are believed to be inadequate.

At the very least, confidential information should always be stored and transmitted in encrypted format. Furthermore, a secure mini-LAN can be established that limits access to the group of individuals immediately involved in the specific transaction, and also tracks and logs specific file access by individual and access point.

Emails and the Internet

Transmission of confidential information by email and email attachment files presents a number of problems. Emails that are embedded in the recipient's email directory must first be labeled appropriately as "confidential" in all subject fields. Because emails can be

stored in multiple locations, this will help ensure that the emails can be identified and then deleted if a transaction is not completed.

In order to better maintain the confidentiality of information and safeguard against possible misdirected emails and fax messages, the parties should specifically name a limited group of persons to whom confidential information may be sent, listing their individual email addresses and fax numbers (and whether their fax is computer based). This can be easily accomplished in an exhibit to the acquisition confidentiality argument. In all emails, the parties should also use a confidentiality banner or disclosure statement (which is now widely used with faxes) noting that the email is confidential, intended only for the named recipient, and may contain information that is legally privileged.

The discloser of confidential information may well decide to conduct an audit of the recipient's security procedures.

While such banners are often appended to the end of email messages, as a practical matter, given the nature of email messages and the fact that a recipient must scroll through them to read them, it makes more sense to place such banner at the very top of the email message. If notification features are available through the sender's email system, the sender should request and, upon receipt, store message opening notifications to confirm delivery to the appropriate address of email messages (similar to how fax transmission confirmation sheets are used). The sender also should request that any unintended recipient immediately delete the email message from his or her computer. Furthermore, the sender also should request that any unintended recipient immediately notify the sender through reply email of the erroneous transmission, thus allowing the sender the opportunity to audit the trail of the message and, if system access is granted, delete any system copies.

As a side note, the Federal Trade Commission's Bureau of Competition has also expressed concern that a "sham" acquisition proposal could be used as a method of exchanging pricing information between competitors in violation of price-fixing laws, and has indicated that, beginning with acquisition confidentiality agreements, appropriate limitations should be set as to who may receive and review confidential and proprietary information.

Back-Up Tapes

Most companies back up data on their computer systems daily, weekly, monthly and/or yearly. If confidential information is saved, in the instances described above, on a yearly backup cycle, that information will remain stored on a tape for one year or until the backup tape is recycled, if in fact it is recycled at all and not simply archived. For example, if confidential customer information is received and stored in a computer file on Monday, the system is backed up on Tuesday, a proposed corporate acquisition is terminated on Wednesday, and the file is deleted from the computer on Thursday, the Tuesday backup tape nevertheless still has the confidential information on it and can be easily restored at any time back onto the computer.

It is impractical, and in some cases impossible, for a company to go back and remove selected confidential information from its archival media. Likewise, it is impractical to expect a company to redeliver or even destroy its archival backup tapes, which often contain huge amounts of data, or not to back up its data at all (unless, of course, a dedicated computer system has been designated for storage of confidential information as such a system is excluded from the normal backup procedures). Furthermore, for emergency reasons, many large financial institutions, securities broker-dealers, and other firms store their backups in offsite facilities where the confidential information may be recovered at a later date.

Standard confidentiality agreements should be updated to require the recipient to conspicuously place a warning on its backup tapes that contain confidential information to the effect that if such tapes need to be restored, the discloser of the information shall be notified and the information shall be immediately erased upon its restoration to disk. In addition, as numerous well-publicized litigations have evidenced, email systems are commonly backed up on a regular basis and confidential email communications should never be overlooked in addressing confidentiality concerns in back up procedures. Likewise, such tapes should be required to be carefully protected through standard physical security restrictions.

File Erasure

Another example of complexity arises when confidential information that has been seemingly deleted can be recovered with various software utilities through "undelete" programs. In order to preserve full confi-

dentiality, confidential files must be erased from the disk or tape itself and not just the link (or pointer) to the files. A number of software programs sometimes create temporary working copies of files that sometimes are deleted automatically, but other times remain on the computer system.

It is important that the scope of "confidential information" be defined broadly to include information in printed form or stored in digital or analog form.

Computer systems should be audited on an ongoing basis to remove temporary, or working, copies of confidential files. Acquisition confidentiality agreements should indicate the file erasure standards to be followed. For example, specific software file utilities are readily available in the commercial marketplace that offer various levels of deletion security including military-level deletion capability so that the sectors on which a deleted file was stored are overwritten with random data one or more times to ensure that no confidential data can be recovered from those data sectors. Furthermore, as an added security measure to prevent the recovery of data from working or temporary files that have been erased, the free space on computer disks that contained confidential files should also be erased using a utility that overwrites the free space on the disk.

Defining Computer Media

Finally, from a legal standpoint, it is also arguable whether the term "copy" includes a computer file in electronic form, or whether it can be considered a copy only when it is printed as a hard copy. This is analogous to oral disclosure, which must be reduced to writing in order to be protectable. It is important, therefore, that the scope of "confidential information" be defined broadly to include information in printed form or stored in digital or analog form, whether on electronic and magnetic media, and pictures thereof stored on film or tape, or electronically stored. Acquisition confidentiality agreements that do not define the information to which they pertain may be an insufficient form of protection because recipients of such information may claim that they were unaware that specific forms of information or media were considered subject to the prohibitions of confidentiality.

Post-Transaction Security Audit

Given the complex nature of the means by which confidential information is exchanged and stored, and the simple fact that no acquisition confidentiality agreement can fully anticipate the full range of possibilities, an additional protection that may be added to such agreement is a provision for a security audit. In addition to requiring the recipient to return all confidential information, the discloser may provide that the recipient will allow the discloser to conduct a security audit following a failed transaction to ensure to the discloser's satisfaction that all disclosed confidential information on the recipient's computer systems has been erased, returned or adequately protected. As a practical matter, if such a provision is accepted by the recipient at the onset of negotiations, it may also serve to encourage diligent compartmentalization of confidential information by the recipient on an ongoing basis to limit the scope of any post-transaction access to the recipient's systems.

Conclusion

While no contractual provision or even diligent practical measures can fully protect a company against the misappropriation of confidential information, disclosers of confidential information should take affirmative steps to safeguard their technology-based confidential information by understanding the possible problems and by building these new protections into their standard acquisition confidentiality agreements. It is also important for the discloser of confidential information to assess how well the recipient protects its own confidential information. In some fields and depending on the nature of the information being provided (whether, for example, financial, technical, or human resource data is involved), added security procedures will be considerably more onerous than necessary. In other instances involving Internet and information technology companies, the procedures may fall short. At the very least, these added security procedures may well impress a potential acquisition partner and serve as an indication of both the company's professionalism and how highly it values its confidential and proprietary information.

SPENCER G. FELDMAN

Spencer G. Feldman is a corporate shareholder in the New York City office of Greenberg Traurig. He concentrates his practice in the areas of public offerings, venture capital and other private financing, and mergers and acquisitions, with an emphasis on representing computer, internet and other technology companies. Mr. Feldman serves as counsel to a number of emerging high-tech business ventures, including companies involved in multimedia and video conferencing, document image processing, point-of-sale computer manufacturing, internet dispute resolution and computer telephony, and regularly participates in counseling the firm's technology clients in connection with raising capital.

Mr. Feldman is currently serving as a member on the Federal Regulation of Securities and Negotiated Acquisitions Committees of the Section of Business Law of the American Bar Association, and is also a member of the New York State Bar Association's Business Law Section. He has authored numerous articles on securities and corporate law issues involving high-tech companies, including Use of Performance (Not Economic) Earn-Outs in Computer Company Acquisitions, Insights (August 1996), Information Technology Due Diligence and Representations, Insights (October 1998), and Are Your Secrets Safe? Acquisition Confidentiality Agreements in the Internet Age, Profit Magazine (September 1999). Mr. Feldman received his J.D. in 1987, *magna cum laude*, from the State University of New York at Buffalo School of Law, where he was an editor of the Buffalo Law Review and received the Laidlaw Award for excellence in all areas of commercial law. Mr. Feldman received his B.A. in 1982, *cum laude*, from Brandeis University. Mr. Feldman is admitted to practice in New York.

INSIGHTS

THE CORPORATE & SECURITIES LAW ADVISOR

Volume 12, Number 10, October 1998

Information Technology Due Diligence and Representations

In the mergers and acquisitions context, buyers need to focus on obtaining representations concerning the target company's information systems. They should also make information technology a priority in their acquisition due diligence.

By Spencer G. Feldman

Stories of companies that have run aground as a result of information technology problems litter the media landscape. One recent high-profile example, Oxford Health Plans, Inc., grew its membership tenfold from about 270,000 members in 1993 to nearly 2 million by 1998. Along the way, it assembled a hodgepodge of different computer systems which, in 1997, the company sought to integrate and upgrade into a new uniform system. What apparently resulted was mismanagement of this process; the system seemed to inaccurately process claims and claim payments, and this led to inaccuracies in Oxford's profits. More recently, Snap-On, Inc., revealed in July 1998, that its second quarter earnings would fall below the prior year's second-quarter results, due in part to systems problems associated with its many acquisitions.

These stories illustrate that, in the mergers and acquisitions context, buyers need to focus on obtaining representations regarding the accuracy of the target company's information systems. When acquiring companies, businesses, technologies or expertise, the purchaser must know what it is acquiring. In today's world, information stored in computer systems plays a key role in the success of businesses. Yet, fast-growing companies like Oxford sometimes neglect to properly maintain their computer systems. Since information technology is not their core business, these companies may make decisions with the best intentions for business growth but which may ultimately impair realization of this goal.

Information Technology Due Diligence

In any merger or acquisition, learning about the target company's computer system should lead to significant insight about the company and its business and financial condition as a whole. For example, the question of whether the target company's software is Year 2000 compliant must be answered, with the purchaser understanding the significance of any non-compliance and the estimated expenditures required to make it Year 2000 compliant. Public companies are already required by the Securities and Exchange Commission to make these and other related disclosures to their stockholders.[1]

In addition, the serious nature of hackers breaking into computer systems has opened many information technology managers' eyes. Any network connection to outside of the company has the potential of a breach of security. A target company should disclose all remote access into its corporate system, including ftp (file transfer protocol), http (hyper text transfer protocol), e-mail, file and fax servers and all dial-up and dedicated telecommunications lines, and whether it uses firewall software. Another area of interest is whether the target company has instituted EDI (electronic data interchange), or extranets, with suppliers or customers. EDI may give external organizations access to a company's internal data and information.

Finally, Web development and Web hosting should be reviewed, as they are typically performed by third parties. Special functionality of a target company's Web site should also be examined. The failure to assure that these arrangements, together with the proper transfer of the target company's software applications, could re-

(Continued on page 3)

Spencer G. Feldman is a shareholder in the New York, N.Y., office of Greenberg Traurig.

A Technology Representation

(Provided by Spencer G. Feldman)

Internal Software Applications

1. ***Software Applications; Year 2000.*** The current software applications used by the Company in the operation of its business are set forth and described on Schedule 1 hereto (the "Software"). Except as otherwise noted on Schedule 1, all of the Software used by the Company complies with the necessary requirements to function efficiently after the year 2000, and is otherwise "Year 2000 Compliant." A description of any non-compliance software and an estimate of the capital expenditures necessary to make such software "Year 2000 Compliant" is set forth on Schedule 1 hereto.

2. ***Owned Software.*** To the extent that any of the Software has been designed or developed by the seller's or the Company's management information or development staff or by consultants on the seller's or the Company's behalf, such Software is original and capable of copyright protection in the United States, and the Company has complete rights to and ownership of such Software, including possession of, or ready access to, the source code for such Software in its most recent version. No part of any such Software is an imitation or copy of, or infringes upon, the software of any other person or entity, or violates or infringes upon any common law or statutory rights of any other person or entity, including, without limitation, rights relating to defamation, contractual rights, copyrights, trade secrets, and rights of privacy or publicity. Neither the seller nor the Company has sold, assigned, licensed, distributed or in any other way disposed of or encumbered any of the Software.

3. ***Licensed Software.*** The Software, to the extent it is licensed from any third party licensor or constitutes "off-the-shelf" software, is held by the Company legitimately and is fully transferable hereunder without any third party consent. All of the Company's computer hardware has legitimately licensed software installed therein.

4. ***No Errors; Nonconformity.*** The Software is free from any significant defect or programming or documentation error, operates and runs in a reasonable and efficient business manner, conforms to the stated specifications thereof, and, with respect to owned Software, the applications can be recreated from their associated source codes.

5. ***No Bugs or Viruses.*** The Company has not knowingly altered its data, or any Software or supporting software which may, in turn, damage the integrity of the data, stored in electronic, optical, or magnetic or other form. Except as set forth on Schedule 1 hereto, the seller has no knowledge of the existence of any bugs or viruses with respect to the Software.

6. ***Pass-Through Warranties.*** The Company shall, to the maximum possible extent, pass through to the purchaser all manufacturer's and supplier's warranties and support contracts for the Software that are not owned by the Company, and the Company shall, upon the purchaser's reasonable request, execute each and every document that is necessary or appropriate to effectuate the purchaser's obtaining and enjoying the benefits of any such pass-through warranty.

7. ***Documentation.*** The Seller has furnished the purchaser with true and accurate copies of all documentation (end user or otherwise) relating to the use, maintenance and operation of the Software.

8. ***Internet Web Site.*** Schedule 8 hereto sets forth the physical location of the computer server which is currently hosting the Company's Internet Web site. Such server is validly owned or a portion is validly leased by the Company. The applicable Internet hosting contract, which describes the Company's contractual obligations, term of the contract, associated costs, corporate information of the host and amount of bandwidth to which the server is connected to the Internet has been previously provided to the purchaser. Schedule 8 hereto additionally sets forth (1) the name and IP address of the Internet Web homepage, when the homepage was granted and the date of the next annual payment, (2) a list of any and all software which can be downloaded from the Web site, and (3) a list of any license agreements displayed on the Web site prior to downloading any particular software. The Company's Web site contains all legal disclaimers believed to be required.

Continued from page 1

sult in the purchaser's inability to maintain and upgrade its information technology following the acquisition.

Technology Representation

To highlight these and other issues, a technology representation in merger agreements and other acquisition agreements is necessary. A suggested form of such a representation is illustrated in the box on page 3. This representation may duplicate parts of other traditional representations (*e.g.*, "Books and Records," "Intellectual Properties," "Approvals and Consents," and "Title Properties"), but in most cases, it goes well beyond the customary "Intellectual Properties" representation since most software is not registered under federal copyright law.

Software Applications

Paragraph 1 of the representation requires the identification of the software used by the target company in the operation of its business. It also, in a very simple way, addresses the Y2K status of the company's software, which should apply to both internally-developed and licensed software. In acquisitions involving industries with particular Y2K sensitivity, such as healthcare, it may be desirable to add a definition of "Year 2000 Compliant," as follows:

> 1. the functions, calculations and other computing processes of the Company's proprietary software, including without limitation all applications and formats (collectively, "Processes") perform in a consistent manner regardless of the date in time on which the Processes are actually performed and regardless of the date of input to the Company's proprietary software, whether before, on or after January 1, 2000, and whether or not the dates are affected by leap years;
>
> 2. the Company's proprietary software accepts, calculates, compares, sorts, extracts, sequences and otherwise processes date inputs and date values, and returns and displays date values, in a consistent manner regardless of the dates used, whether before, on or after January 1, 2000;
>
> 3. the Company's proprietary software will function without interruptions caused by the date in time on which the Processes are actually performed or by the date of input to the Company's proprietary software, whether before, on or after January 1, 2000;
>
> 4. the Company's proprietary software accepts and responds to two-digit year-date input in a manner that resolves any ambiguities as to the century in a defined, predetermined and appropriate manner; and
>
> 5. the Company's proprietary software stores and displays date information in ways that are unambiguous as to the determination of the century.

Owned Software

In the absence of federal trademark, copyright or patent registration, it is important to include, as provided in paragraph 2, firm representations regarding ownership, rights to possession and non-infringement representations, and to provide that the company has not otherwise licensed or distributed the software to any other person. From an organizational point of view, purchaser's counsel may also find it helpful if the seller lists its owned software and licensed software separately on the disclosure schedules to the acquisition agreement.

Licensed Software

The representation in paragraph 3 relates to licensed software, whether licensed privately or purchased "off-the-shelf" at a retail store. Paragraph 3 is intended to provide assurance that the transfer of the software will not violate applicable licenses. In addition, the representation in the second sentence of paragraph 3 covers both instances in which unlicensed or "pirated" software is being used and instances in which otherwise licensed software is being used at multiple stations in violation of a defined CPU (central processing unit) or user license. Damages at law could be substantial in these instances, and licensors have been known to make unannounced spot inspections. In addition to making their own inspections, major United States software producers have formed organizations, such as the Business Software Alliance and Software Publishers Association, whose purpose is to vigorously seek out and take enforcement action against users of unlicensed copyrighted software.

Nonconformity

The operation of the software also needs to be addressed in the representation. In paragraph 4, the seller should represent and warrant that there are no software

defects or documentation errors and that the software conforms to its specifications. From the seller's perspective, counsel may request a "knowledge" qualifier to this representation or seek to narrow its application to only internally-developed software. Finally, the synchronization of the software application and its associated source code should not be overlooked. If the executable version of the software is lost or destroyed, the program must be able to be recreated exactly from the source code.

No Bugs or Viruses

The representation in paragraph 5 covers, in an acquisition which is less than friendly, an intentional insertion of a "bug" or "virus" in the software that could later cause data loss or corruption or abnormal "crashing" of the program or the entire computer system. Because a "virus" will not show up until a later time, this representation should survive the closing for, ideally, up to three years. Additionally, based on internal software bug or "trouble" reports, the seller should be able to detail any bugs which currently exist in the software.

Pass-Through Warranties

In instances where the software is licensed from a third party, paragraph 6 provides that all manufacturer and supplier warranties and support contracts running to the seller should be passed through to the purchaser. Often, software license agreements will require the licensor's prior written consent to assign, and the seller should cooperate by executing any agreement or taking appropriate actions to effectuate the transfer of the license.

Documentation

The representation in paragraph 7 is necessary, particularly where internally-developed and customized software is being used, due in many cases to the complexity of such software.

Internet Web Site

As noted above, the representation in paragraph 8 addresses Web development and Web hosting, which are not usually done internally and may be overlooked in the customary "Contracts and Commitments" representation. Through this disclosure, the acquiror should discover special features and functions of the Web site including ftp, IP telephony and the information that may be downloaded to a Web visitor's personal computer (known as "cookies").

Personnel Confidentiality

In an asset transaction, a purchaser may also wish to further establish and protect its rights against unauthorized disclosure and use of the software by non-retained personnel of the seller. In such case, the purchaser should request that the seller cause certain of its personnel to enter into confidentiality and non-disclosure agreements for the purchaser's benefit on or before the closing of the acquisition.

Conclusion

Tremendous effort is spent by companies on mergers and acquisitions from performing due diligence to finalizing a purchase agreement's representations and warranties, but sometimes little attention is paid to information technology issues. Failure to appreciate the importance of information technology in this overall process could have substantial adverse consequences and potentially wipe out any hoped-for synergies of an acquisition. Companies that make information technology a priority in their acquisition due diligence will get more out of the deal.

Note

1. *See, e.g.*, Release No. 33-7558 (July 29, 1998), effective August 4, 1998, and other materials referenced on the SEC's homepage at *www.sec.gov/news/home 2000.htm*.