

2008 BUSINESS LAW ANTHOLOGY

NICOLAI LAW GROUP, P.C.
BUSINESS LAW & LITIGATION

Tarbell-Watters Building
146 Chestnut Street
Springfield, Massachusetts 01103-1539
www.niclawgrp.com
Telephone: 413.272.2000 • Facsimile: 413.272.2010

NICOLAI LAW GROUP, P.C.

BUSINESS LAW & LITIGATION

Caroline E. Nicolai, Esq.,

Direct Dial Extension 224

E-MAIL Address:

CAROLINE.NICOLAI@NICLAWGRP.COM

Tarbell-Watters Building

146 Chestnut Street

Springfield, Massachusetts 01103-1539

Internet: WWW.NICLAWGRP.COM

Telephone: 413-272-2000

Facsimile: 413-272-2010

I am pleased to enclose our **2008 BUSINESS LAW ANTHOLOGY**, a collection of the legal memos our business customers received as part of our service to them.

These memos are examples of where Nicolai Law Group professionals concentrate. Complex business issues are where our experience and value are most effective and provide customers the best value.

Beside a number of multi-million dollar financings and acquisitions, our engagements include:

- Negotiating multiple commercial leases for multi-unit operation rollouts.
- Restructuring equity and debt portfolios for several large operations.
- Negotiating joint venture arrangements for several clients including multinational manufacturing and distribution arrangements.
- Negotiating project contracts for clients nationally.
- Successful litigation of employment and other matters in several states.
- Arbitration of dozens of matters involving business arrangements, intellectual property issues and multi-party contractual arrangements.
- Negotiation of several international software development agreements.

In addition, we are pleased to announce the election of Paul Nicolai as a **2009 Best Lawyer in America for Commercial Litigation**; that he participated as as panel member at the **ABA Center for Professional Responsibility 24th National Forum on Client Protection**, authored **AFTER THE AWARD** for the Massachusetts Bar Association and was nominated to the **Strategic Planning Committee of the ABA Center For Professional Responsibility**.

When there is a strategic need for counsel in complex business litigation and deal issues, we hope to be among your first sources. Whether we can help or not, we're always happy to share information and contacts to set you on the right course.

Sincerely yours,

Caroline E. Nicolai

Caroline E. Nicolai

2008 BUSINESS LAW ANTHOLOGY

TABLE OF CONTENTS

Defined Contribution Plan Liability Upped.....	1
E-Discovery Dawns.....	3
Antiboycott Voluntary Self-Disclosure	6
Electronic Mail Message Retention	11
New Employment Arbitration Rules.....	22
The Hidden Franchise	26
Internet Job Application Recordkeeping	31
Maintaining Your Corporate Veil.....	35
Open Source Code	38
Trademark & Trade Secret Record Retention.....	42
Shareholder Liability for Copyright Infringement.....	49
Succession Planning Benefits & Risk Management.....	53

Defined Contribution Plan Liability Upped

Until a recent US Supreme Court decision, defined contribution “account” plan holders subject to ERISA could only sue to recover their plan account balance or get “appropriate equitable relief” if a problem arose that affected the account. Courts refused to order monetary relief on the ground that it was not equitable relief. That view changed in the Supreme Court's LaRue decision. The Court held individuals covered by 401(k) and similar plans can get money damages if their plan account suffered a loss because of a breach of duty or a statutory violation by a plan fiduciary. The Court declined to give lower courts direction beyond saying such lawsuits are possible.

There has been a surge in lawsuits under ERISA. Most involve defined contribution plans, the predominant form of ERISA regulated plan. These plans have a signature feature of a plan “account.” Each plan-covered individual has their own account to which contributions, gains and losses, and income and expenses are credited. The fundamental problem with maintaining an account through this type of plan is that it exposes the account owner directly to investment risk. If the account does well, the individual benefits. If the account does poorly, the individual suffers. Inevitably, the individual's prospects at least partly depend on how the plan's fiduciaries discharge their responsibilities.

WHAT LARUE DECIDED

ERISA permits plan covered individuals to sue to recover contracted for benefits; to recover losses “on behalf of” the plan that result from a fiduciary breach or a violation of ERISA's minimum standards; and to recover appropriate equitable relief if ERISA rights have been violated or need to be safeguarded.

Section 502(a)(2) potentially provides the broadest relief because it can be used to hold a plan fiduciary personally liable for any monetary loss the fiduciary caused through a breach of duty or unlawful conduct. Courts in the past have prevented individuals from bringing suit under §502(a)(2) because the lawsuit has to be brought “on behalf of” the plan itself. Those decisions were particularly unsatisfying when a this kind of plan was involved because, from the perspective of an individual covered by a DC plan, their account is the plan. In LaRue, the Supreme Court recognized that proposition.

In this case, a participant in a 401(k) plan brought a claim against the plan's administrator seeking money under §502(a)(2), alleging that its failure to carry out his instruction to sell and buy some of the investments in his account was a breach of fiduciary duty that caused him to lose \$150,000. The participant

sued under §502(a)(2) because he could have recovered only his account balance by suing under §502(a)(1), and suing under § 502(a)(3) would have qualified him for only injunctive or similar relief. The lower courts dismissed the claim on the grounds that §502(a)(2) provides remedies only for claims brought “on behalf of” the entire plan. The Supreme Court reversed, unanimously holding that an individual covered by such a plan may bring a claim for a breach of duty under §502(a)(2), even if his is the only account affected by the breach. The Supreme Court stopped there, in part because of an apparent disagreement among the justices over whether permitting individuals to bring such claims under §502(a) (2) creates practical problems for ERISA regulated defined contribution plans.

While holding that individual participants in these plans can sue to recover losses suffered in their plan accounts as a result of a fiduciary breach, the majority acknowledged it could reach its decision only by assuming away important aspects of the case, like whether LaRue had timely asserted his rights and exhausted any right under the plan to subject his claims to an internal review by the plan’s fiduciaries or demand that the plan’s fiduciaries find some way to fix his claimed loss. The concurrence focused on the assumptions and suggested LaRue should have first brought his claim for plan benefits and then sued under §502(a)(1) “to recover benefits due to him under the terms of the plan” to provide the plan’s fiduciaries with the opportunity to resolve any individual loss found to have occurred. ERISA requires all plans to maintain a claims procedure and courts historically have required a plan covered individual to first present his claims to the plan’s fiduciaries under the procedure before bringing suit, unless the individual could show that following the claims procedure would be futile. This signals there are likely to be instances when plan fiduciaries are in a position to resolve an individual participant or beneficiary’s claimed loss, possibly by recouping the loss from a third party (such as a vendor that overcharged the plan or, in a case like LaRue, a broker who failed to execute the trades needed to implement the participant’s investment directions).

The concurrence warned that allowing a plan participant to proceed directly to court by bringing a breach of duty claim would enable the participant to bypass the plan’s fiduciaries rather than give them the opportunity to fix plan problems and resolve competing claims on behalf of the entire plan.

E-Discovery Dawns

Changes have been made to the Federal Rules of Civil Procedure to address the increase of electronic information. They relate to information stored on computers or other electronic media during the discovery part of lawsuits. Before these amendments, whether electronically stored information should be searched or produced was a point of disagreement. The amended rules have resolved the issue. Electronically stored information is discoverable.

Compliance with the new rules is required of all parties to federal litigation. If your business is not involved in a federal lawsuit or anticipating involvement in one, it has no existing obligation. Some states are already in the process of amending their rules to include e-discovery provisions like the new federal rules. You should anticipate your business will soon be subject to state or federal e-discovery rules.

The best practice is to be prepared.

MAPPING & DOCUMENTING

The new rules assume each party knows its computer systems and record retention procedures, and can relay this information as it stands and at the time of the events relevant to the dispute to its attorney in 90 - 120 days from when suit is filed.

To be ready, you should map your computer systems to show how your computers are setup. You should also evaluate your record retention policies. If you have no policy, write one. If you have a policy but don't follow it, redo the policy so it works and is followed. If you have a policy and follow it, audit to confirm compliance. Being able to provide information about your computer systems and record retention policies will give your attorney the tools to comply with the e-discovery rules and begin limiting the scope of discovery with the other side.

Coming to an understanding of your computer systems and record retention environment is best done without the pressure of a lawsuit. The best practice is to map your computer infrastructure and document your retention policies before a lawsuit.

WHEN OBLIGATIONS BEGIN

The e-discovery rules do not say when a business is required to preserve information. Case law says this obligation begins when a lawsuit is reasonably anticipated. This is not a clear definition. In most cases, waiting until a complaint is served is probably too late. On the other hand, not every threat will actually end up in a lawsuit. To assist in this making this decision, you can:

- Learn from past circumstances where litigation did occur. By looking at past litigation, you can narrow down the types of litigation you have encountered.
- Look at past situations where you received a litigation threat that never resulted in a case. For instance, measuring how many employee complaints you got versus how many lawsuits were filed by employees will help you assess the seriousness of such threats.

Using this kind of information, you can develop a set of guidelines for assessing threats. If the threat is in a category of litigation experienced by your business, and the majority of threats of this nature resulted in a suit, a new threat will likely be "reasonably anticipated" litigation. You should document information about the alleged wrongdoing and any decision to begin or not begin saving information. This will both assist in assessing future threats and showing the thought process behind your decision to save or not save and how the decision was reasonable.

Beside guidelines for assessing litigation threats, you should develop a formal plan to respond to reasonably anticipated litigation. It should include a strategy for implementing a legal hold to preserve information once a litigation threat is sufficiently legitimate, and a plan for responding to discovery requests. In larger organizations, a litigation response team should be established. It should include members from a variety of departments like legal, IT, records management, operations, human resources, etc. This team will be responsible for assessing the litigation threat, implementing the litigation hold, and responding to discovery requests.

ELECTRONICALLY STORED INFORMATION IS PRODUCED DIFFERENTLY

Until now, discovery has meant searching, collecting, copying, and submitting paper documents to your attorney for review and production to the other side. The process is different for electronically stored information in key respects. You may see increased litigation costs as a result.

First, you may not be able to pull electronically stored information together as easily as paper. A clerk will not be able to do this. Instead, IT staff will need to locate the potentially relevant electronically stored information. Depending on a number of factors (including not having an IT staff), outside help may need to be hired to collect the electronically stored information.

Expect a much greater volume of electronically stored information than paper. Electronic information is typically stored in numerous places. Work habits don't always mean draft documents were deleted. Because the amount of information may be sizeable, your business may need to filter information not relevant to the case. For example, you may be asked to list the people directly involved with the event surrounding the dispute. You may be asked for infor-

mation from the time of the event in dispute. Temporal and other limits like it can be used to narrow the collection to relevant electronically stored information and reduce the cost.

Once the electronically stored information is collected, it may be produced as is – called native production. For example, if an Excel spreadsheet is collected, it would be produced as an .xls file. Native production has advantages and disadvantages. An advantage is no additional processing is required so processing cost will be less. However, your attorney will spend more time reviewing because it is not possible to search across multiple file types, and your attorney will spend time re-reviewing the same document because it is not possible to remove duplicates. Other disadvantages include an inability to block privileged or confidential information from documents and being unable to view documents without the software used to create documents or a universal viewer.

Another production format is quasi-paper production, or TIFF/PDF production. Here, the information is processed and converted into image files. These image files are loaded into a database for attorney review. With this method, duplicate documents can be removed, privileged information can be redacted, documents can be reviewed without the original creation software, and the reviewer can search across differing file types. The major disadvantage is that processing the information into an image file adds cost, and depending on the volume, may require hiring an outside vendor.

Other forms include traditional paper production and quasi-native production. Quasi-native production is taking information from an original database and transferring it to another database for production. This type of production may be used for information held in proprietary software.

You should decide which format is best for you to produce information to an opposing party and which format is best for you to get information from the opposing party. Knowing this will help in negotiating and agreeing to production formats with the opposing party, something the e-discovery rules contemplate.

If no agreement can be made, the rules have a fall-back provision - either the electronically stored information is produced in native format, or a form that is reasonably usable and searchable.

The rules make it clear that the information on your computers is discoverable. It is time to get ready.

Antiboycott Voluntary Self-Disclosure

The Export Administration Act (EAA) and Export Administration Regulations (EAR) require exporters to report certain boycott-related activities to the Department of Commerce's Office of Antiboycott Compliance (OAC). The EAR general record-keeping provisions apply to antiboycott related situations. Companies need to have effective compliance programs to detect and report the receipt of boycott-related requests. Good records retention practices are an essential part of the compliance program and EAR specifies how companies must act. The records retention requirement says records containing information relating to a reportable boycott request, including a copy of any document(s) in which the request appears, must be maintained by the recipient for five-years after receipt. The Department may require these materials be submitted to it or that it have access to them at any time within that period.

This is not limited to exporters. All "U.S. persons" are covered by this requirement. Thus, banks and other financial institutions, insurers, freight forwarders and manufacturers have to be on the lookout for boycott requests.

As to what requests are reportable, the regulations say that a United States person who receives a request to take any action which has the effect of furthering or supporting a restrictive trade practice or boycott fostered or imposed by a foreign country against a country friendly to the United States or against any United States person must report such request to the Department of Commerce. Such a request may be either written or oral and may include a request to furnish information or enter into or implement an agreement. It may also include a solicitation, directive, or instruction that asks for information or that asks that a United States person take or refrain from taking particular action. Such a request must be reported regardless whether the action requested is prohibited or permissible, except as otherwise provided.

The regulations also say a request received by a United states person is reportable if he knows or has reason to know that the purpose of the request is to enforce, implement, or otherwise further, support, or secure compliance with an unsanctioned foreign boycott or restrictive practice.

VOLUNTARY SELF-DISCLOSURE

In 2007, the Bureau of Industry and Security (BIS) published a new rule on voluntary self-disclosure of violations of the EAR antiboycott provisions. The rule sets forth the factors BIS will consider when deciding whether to pursue administrative charges or settle allegations of violations, and the factors BIS will consider when determining what penalty to seek in administrative cases.

Compliance is important. In July 2007 BIS announced that Dresser Inc. agreed to pay a \$9,000 civil penalty to settle allegations it violated the EAR antiboycott

provisions. BIS alleged that from January 2001 through January 2004, Dresser failed to report in a timely manner its receipt of nine requests to engage in a restrictive trade practice or boycott. The company voluntarily disclosed the transactions and cooperated fully with the subsequent investigation. The transactions involved the sale of goods to Pakistan.

The rule lays out the specific procedures for voluntary self-disclosures. It also describes how BIS responds to violations of the antiboycott provisions and how it makes penalty determinations in the settlement of antiboycott administrative enforcement cases.

The rule defines what is a voluntary self-disclosure and provides the procedures for making them. A voluntary self-disclosure satisfying the rule is designated as a mitigating factor of "GREAT WEIGHT" in settling administrative cases. The rule provides that such factors will ordinarily be given considerably more weight than a factor that is not so designated. In addition to providing an incentive for voluntary self-disclosures, BIS anticipates the rule will promote more effective use of OAC resources, as the receipt of voluntary self-disclosures will reduce the time OAC must spend identifying and investigating possible violations. The rule provides the benefit of a mitigating factor to those who self-disclose before OAC has invested resources to investigate violations based on information it might receive from another source.

The rule requires, among other things, that voluntary self-disclosures be written and received by OAC before it learns of the same or substantially similar information from another source and has opened an investigation or inquiry in connection with that information. A person may make an initial written notification followed by submission of a more detailed narrative account and supporting documents. To determine whether a voluntary self-disclosure was received before OAC learned of the same or substantially similar information from another source, the initial disclosure date will be used if the discloser subsequently submits the required narrative account and supporting documentation. BIS recognizes that two features of its existing regulations may impact the requirement that a voluntary self-disclosure be received before OAC learns of the same or substantially similar information from another source. The first such feature is the reporting requirements in another rule. The second is OAC's practice of encouraging persons with questions about the EAR to contact OAC by telephone or e-mail for advice.

Section 760.5 of EAR requires any U.S. person who receives a request to take any action that would have the effect of furthering or supporting a restrictive trade practice or boycott fostered or imposed by a foreign country against a country friendly to the United States or against any United States person to re-

port to OAC both receipt of the request and the action the person took in response to it. In some instances, taking the requested action would be a violation. BIS recognizes the reporting requirements would have the effect of requiring a person to disclose a violation in those instances. The regulations say reports filed under the rule are "information received from another source." Thus, a person who wishes to make a voluntary self-disclosure of a violation based on an action Section 760.5 requires that person to report, would have to make sure OAC receives the written initial notification of the voluntary self-disclosure before OAC began an investigation based on the information received in the required report. The report itself is not the initial notification. If OAC received the report and the initial notification simultaneously, it would be deemed to have received the initial notification before it had begun an investigation.

OAC has for years provided advice about the antiboycott provisions to persons requesting such it by telephone or e-mail. Sometimes the persons requesting advice may disclose they committed a violation. OAC's practice has been to encourage such persons to make voluntary self-disclosures. OAC wants to continue to encourage persons with questions to disclose all relevant facts when inquiring for advice. The rule provides that violations revealed in telephone or e-mail requests for advice are not information received from another source for purposes of the rule. The rule also says information provided by telephone or e-mail while seeking advice is not a voluntary self-disclosure or an initial notification of a voluntary self-disclosure. OAC's practice is to inform persons who reveal violations when seeking advice of their opportunity to make a voluntary self-disclosure.

The rule also provides that for a firm to be deemed to have made a voluntary self-disclosure, the individual making the disclosure must do so with the full knowledge and authorization of senior management or an officer or employee who is authorized to make such disclosures for the firm. BIS believes approval of a person with such authority is needed to make clear a firm may not claim the benefits of a voluntary self-disclosure when a subordinate employee acting on their own initiative disclosed wrongdoing.

The rule also creates a new Supplement to Part 766, which sets out BIS's practice on violations of the antiboycott provisions. The supplement describes the ways BIS responds to violations, the types of administrative sanctions that may be imposed for violations, the factors BIS considers in determining what sanctions are appropriate, the factors it considers in determining the appropriate scope of the denial or exclusion order sanctions, and the factors considered when deciding whether to suspend a sanction.

The supplement contains BIS's policy of encouraging any party in settlement negotiations with it to provide all information the party believes is relevant to

applying the guidance in the supplement and information relevant to deciding whether a violation has occurred and whether the party has a defense to potential charges.

The supplement lays out the three actions BIS may take in response to a violation; issuing a warning letter, pursuing an administrative case, and referring a case to the Department of Justice for criminal prosecution. It also lists the factors that often cause BIS to issue a warning letter. It also notes BIS's ability to issue proposed administrative charging letters instead of actual charging letters. Proposed letters are issued informally to provide an opportunity for settlement before a formal administrative proceeding. BIS is not required to issue a proposed charging letter. BIS may refer a case to the Department of Justice for criminal prosecution in addition to pursuing an administrative enforcement action.

The administrative sanctions that may be imposed in antiboycott administrative enforcement cases are: A monetary penalty, a denial of export privileges and an order excluding the party from practice before BIS.

Information about how BIS determines what sanctions are appropriate in settling antiboycott administrative enforcement cases is also provided. There are both general factors and specific mitigating and aggravating factors. BIS typically looks to the specific factors, alongside the general factors, in determining what sanctions should apply.

Seven general factors BIS looks at are: Degree of seriousness, category of violation, whether multiple violations arise from related transactions or unrelated transactions, the timing of settlement, whether there are related civil or criminal violations, and the party's familiarity with the antiboycott provisions. There is general guidance on how BIS applies each of these general factors.

The role of eight specific mitigating and nine specific aggravating factors whose presence or absence is generally considered is also discussed. BIS may consider other factors in a particular case, however, the listed factors are those experience indicates are commonly relevant to penalty determinations in settlements. Factors identified with "GREAT WEIGHT" will ordinarily be given considerably more weight than other factors.

The eight specific mitigating factors are: Voluntary self-disclosure, having effective compliance program, limited business with or in boycotted or boycotting countries, history of compliance with the antiboycott provisions, exceptional cooperation with the investigation, a lack of clarity of the request to furnish prohibited information or take prohibited action, violations arising out of a

party's passive refusal to do business in connection with an agreement, and isolated occurrence.

The nine specific aggravating factors are: Concealment or obstruction, serious disregard for compliance responsibilities, a history of lack of compliance with the antiboycott provisions, familiarity with the type of transaction at issue in the violation, prior history of business with or in boycotted countries or boycotting countries, long duration or high frequency of violations, the clarity of the request to furnish prohibited information or take prohibited action, violation relating to information concerning a specific individual or entity, and violations relating to active conduct concerning an agreement to refuse to do business.

BIS believes that in most cases, evaluating these factors provides a fair basis for determining the penalty appropriate when settling an antiboycott administrative enforcement case.

BIS also lists the factors it considers particularly relevant when deciding whether to impose a denial or exclusion order in the settlement of antiboycott administrative enforcement cases. The four factors given great weight, degree of seriousness and history of prior violations and their seriousness are included. In addition, BIS considers the extent to which a firm's senior management participated in or was aware of the conduct that gave rise to the violation, the likelihood of future violations, and whether a monetary penalty could be expected to have a sufficient deterrent effect to be particularly relevant in determining whether a monetary penalty is appropriate.

BIS also provides examples of factors it may consider in deciding whether to suspend or defer a money penalty or suspend an order denying export privileges or providing for exclusion from practice. With respect to suspension or deferral of money penalties, BIS may consider whether the party has demonstrated a limited ability to pay an appropriate penalty so that suspended or deferred payment can have sufficient deterrent value, and whether the impact of the penalty would be consistent with the impact of penalties on other parties committing similar violations. On suspending denial or exclusion orders, BIS may consider the adverse economic consequences on the party, its employees and others, as well as on the national interest in the competitiveness of US businesses. Such orders will be suspended for adverse economic consequences only if future violations are unlikely and if there are adequate measures (usually a substantial civil penalty) to achieve the necessary deterrent effect.

Electronic Mail Message Retention

Email use is growing exponentially. In 2005, the average user processed 75 emails a day. Corporate email traffic per user has increased 33% per year since then. Worldwide traffic in 2006 was 183 billion messages a day.

Many organizations are struggling to decide how to cope with the email explosion while reconciling competing needs imposed by business, regulatory and litigation requirements. Although the legal, regulatory and cultural environment in organizations vary greatly, there are common elements to a legally defensible email management policy. The key is a good faith development and enforcement of reasonable policies that best fits the entity.

GUIDELINES

Guideline 1: Email retention policies should reflect the input of functional and business units through a team approach and include the entire organization including portions outside the United States.

Guideline 2: The team should develop an understanding of email retention policies and practices actually used in the entity.

Guideline 3: An entity should select features for updates and revisions of email retention policy understanding that multiple approaches reflecting size, complexity and policy priorities are possible.

Guideline 4: Any technical solution should meet the functional requirements identified and should be carefully integrated into existing systems.

FRAMEWORK FOR POLICY DEVELOPMENT

General Retention Considerations

A business has responsibility and authority to decide how to use and retain information managed by its email system. This includes deciding on features that impact the duration of email retention. An organization need not retain all electronic information ever generated or received. An email retention policy may be independent of other retention policies or it may be part of an umbrella policy on “records” or “document” management.

Email retention policies must be reasonable in purpose and application. They must take into account statutory and regulatory mandates that directly or indirectly govern email management in your operation. The policy must recognize the need to preserve and produce information sought in legal proceedings.

For example, the financial services industry is governed by detailed regulations impacting information system operation. State, federal and local public entities

are often also required to manage information created by or received on email systems in accordance with specific regulations.

Typical Retention Features

Email retention policies today frequently include some or all of the following features to maintain efficient operation. The focus is on management of email on active sources accessible to users inside a firewall that provides appropriate security, virus protection and reasonable spam protection.

1. User Quotas

Quotas on the storage available to a user has historically been a principal feature of email management. In a 2005 survey, over one half reported they were “managing” email retention by limiting mailbox sizes. Quotas can vary widely. Typically, a user is given a warning before email is deleted, although the ability to send or receive email may be automatically disabled pending reduction below size limits.

2. Automatic Content Deletion

Many entities automatically delete email after it has been retained for a number of days. Typically, this policy is tied to options so users can move email of significance to an appropriate alternative storage location. Some users are required to print and file email and attachments into a records management system. Some require users to assign individual retention durations to email. Yet another approach is to delegate the responsibility to the user to set up and use a local file structure which mimics existing records retention schedules for that unit.

Automatic classification of email by content using computer generated criteria is not yet a proven technique for managing retention.

Some types of email content (relating to contracts, regulatory files, trade secrets, and critical business records) may be sufficiently important that dedicated electronic content management repositories are also made available.

3. Extended Storage Options

Some entities provide extended capacity or archival storage for undeleted or unallocated email. Email not deleted by a user within a certain period may thus be saved for a long period, with decisions on moving individual email to records management postponed to another day.

Entities doing this typically move email from active servers to lower cost storage that offers capacities like message de-duplication to reduce server use. A variation is to put email into a “vault” or “safe” where the user cannot change or delete the information but can continue to access it. This increases the likelihood information will be accessible when needed. Advocates of this approach

argue implementation of litigation holds involving large numbers of custodians can be more easily and uniformly managed by this feature.

Some entities confine this strategy to specific groups - like scientists, executives, accountants and HR representatives - because their information predictably may be needed for future business or regulatory inquiry. For these groups, an outer limit of retention may be established based on the various regulatory and business retention requirements. These requirements stem from a large set of statutes, regulations and other business requirements.

A variety of practices exist on assigning retention periods. Some require users use existing records schedules. Others develop highly simplified versions of their records schedules specifically for individual email based on content. Others assign uniform, long term retention periods to all email for classes of users or departments without individual classification.

4. Restrictions on Local Storage

Some prohibit users from placing information on local drives or other distributed devices to avoid the problem that they cannot be accessed by others and are not backed up. Eliminating this option can be controversial since some users feel local storage is essential to their productive use of information.

The Importance of Litigation Holds

A good faith and reasonable effort to implement a litigation hold to preserve potentially discoverable information needed for litigation or government investigations must be made once a preservation obligation is triggered.

Email retention policies must take this into account. Courts have imposed sanctions where email was destroyed or lost when a preservation obligation was in effect. Generally, courts have broad discretion in setting sanctions for what is called spoliation.

2006 Amendments to the Federal Rules of Civil Procedure do not specially spell out when or how a preservation obligation for email is triggered. They also do not identify the exact scope of the duty and how it is satisfied. Parties are encouraged to assess and discuss preservation issues early. Rule 37(f) provides for limited protection from some sanctions based on the presence of routine, good faith operations of information systems.

Emerging case law shows that the litigation holds on email will receive high scrutiny. Reasonable care must be taken administering a litigation hold to ensure that routine features that interfere with preservation are dealt with.

The email retention policy may leave the specific details of litigation hold implementation to other policies and procedures, but it is important to be able to

demonstrate that email retention practices are actually subject to the constraints imposed by preservation obligations as they arise.

DISCUSSION

Guideline 1: Email retention policies should reflect the input of functional and business units in a team approach and should include the entire organization including any operations outside the United States.

Email management was viewed primarily as something handled by the IT department on advice from the legal department. Confusion and frustration by users and developments in litigation has led to some dissatisfaction with that approach. It is more typical of current practice for a team of both functional and user representatives to be assigned to assess an email retention policy. The assessment should include representatives of Legal, IT, Records Management, Compliance, Finance, and representatives of major business units - domestic and international. Complex issues are involved when an entity operates inside and outside the United States because its email system typically encompasses the whole enterprise. The entity might decide to use a decentralized email retention approach under the umbrella of a single broad policy with individual national policies corresponding to organizational units. The team is often empowered to assess the current status of policy and make recommendations on changes, if any, that may be deemed necessary or desirable, including development of new policy features.

The team should be empowered to use the expertise of consultants, professional organizations, outside lawyers and vendor representatives. A decision should be made as to what departments or units are going to be primarily responsible for developing, implementing and monitoring email retention policies for the functions or enterprise as may be applicable to the entity. A fully engaged, responsible person should be appointed to lead the team to work closely on implementation, including recommendations on budget and monitoring the program after implementation.

Guideline 2: The team should develop an understanding of email retention policies and practices actually used in the entity.

It is important the team understand the email management policies and practices actually in place that may relate to retention. The goal is to identify the practical gaps, if any, between existing policies and actual practices and the costs and risks present. The results can be used in discussions of proposed changes or revisions under consideration.

It is important for the team to develop an understanding of these basic background questions:

- What are the current policies, processes, work practices, or procedures applicable to the creation, distribution, retention, retrieval, and deletion of email and other electronic communications?
- What contextual information does the email system generate?
- What types of personal or distributed electronic devices are used for handling email?
- What types of content are transmitted or received by email or contained in message bodies?
- What user management practices are encouraged or tolerated for individual email accounts?
- What access to personal email archives exist on local hard drives and how often are they used?
- What is the user's role in deciding how long email is kept?
- When and how are existing policies and procedures communicated to users?
- Who in the organization is responsible for or has email policies in place?
- How does the organization define a "record" and to what extent are emails, usually based on content, included in this definition?
- How are emails with business significance, as defined by records schedules, treated?
- What are the current audit practices and capabilities to assure system integrity?
- Are users required to ascertain and classify email and to what extent is this accomplished?
- How is email integration into records management systems accomplished?
- How are litigation holds applied to email?

It may be useful to retain an outside consultant to help perform this assessment. The review of existing policies and interviews should include focus groups and surveys, including benchmarking exercises or

other informal methods of developing comparative examples of possible policy features in larger organizations.

As a starting point, IT should brief the team on the relevant technology and storage architecture, including all storage locations or potential “sources” of email and attachments. Close attention should be paid to understanding the actual functioning of the active and backup email systems and the policies and practices relating to any backup media used.

The team should become aware of the relevant legal principles governing the use and retention of email, with some focus on the organization’s particular litigation environment. This could include a review of the types of repetitive litigation encountered, practices followed in preserving accessible and inaccessible sources of information in contemplation of discovery in litigation, and the process followed in identifying and producing email and other information for discovery, together with any costs, burdens, and problems encountered in carrying out the discovery process.

Finally, the records management function should be asked whether email and attachments are currently expected to be reviewed for content and incorporated into records management storage policies and practices. The unique regulatory, business and legal requirements applicable to an entity play an important role in deciding what reasonable practice is.

With this input, the team can develop an accurate evaluation of the effectiveness, business needs, costs and risks associated with current practices to help set the stage for an analysis of the need, if any, for revisions in existing policies and practices.

Guideline 3: An entity should select features for updates or revisions of email retention policy with the understanding that a variety of possible approaches reflecting size, complexity and policy priorities are possible.

Selecting the right retention strategy for active email in use is the primary focus of any review. In some cases, this may result in only establishing additional processes or features to strengthen existing policy. Sometimes it may involve significant revisions or the development of a completely new strategy. The unique experiences of the entity within its context will govern this.

Reaching consensus in the face of differing objectives of different representatives is not easy. The team members should be encouraged to openly discuss their differences of viewpoint and identify why they believe them to be important.

Each goal or objective should be assessed in the context in which the entity operates. Costs and risks associated with change are often a limiting factor. Perceived benefits may not be worth the effort and investment required. The risks associated with any particular goal should also be carefully assessed.

Default Retention Strategy

One place to start is developing a consensus on the duration of continued access - the “default retention strategy”. There are sharply contrasting practices on this. Some focus strategy on quickly reducing the volume routinely accessible to users from active sources. The key philosophy is that email with only “transitory” information of no lasting value is quickly eliminated. This approach requires paying careful attention to implementation of a litigation hold process. Any approach that emphasizes short email retention should also provide alternative storage to enable the retention of information with longer-term value.

Another approach is to permit email retention at user discretion with outer limits. Here, the argument is that accurate assessment of individual email value cannot always be made when created. Some argue classification decisions by users are rarely consistent and risk exposing the entity to loss of needed information. They believe the best way to maximize productivity is to allow users to continue to have access to information, regardless of its perceived age or value.

This approach can be expensive and difficult to implement and has the drawback of increasing the information stored and which must be searched and reviewed during litigation.

Choosing Features

After discussing a basic retention strategy and the related general objectives, the team can seek a consensus on the specific features included in the email policy. To focus discussion, an attempt should be made to benchmark with similar sized organizations to see what they have found useful, taking their strategy into account. Identifying features and assessing risks and values should involve the full team and be done thoroughly. Naturally, legal and regulatory advice will be crucial, but the full team should participate.

Once adopted, implementing the policy will require careful and focused attention. Typically, it will be rolled out through targeted training and the use of internal web resources as part of compliance initiatives.

Guideline 4: Any technical solutions should meet the functional requirements identified as part of the policy development and carefully integrated into existing systems.

A revised policy may require additional software or hardware. These decisions involve important technical issues, including integration with existing systems. Care should be taken to ensure technology is selected to meet specific goals and that policy and work practices are not being changed only to match available technology. Any assessment of the suitability of products should be driven by business, technical and records management considerations.

Among the issues that should be examined are:

- Ability to be integrated into your technology infrastructure and existing work practices
- Ability to efficiently and accurately search and retrieve information
- Technological assurance, including experience, scalability and performance
- Ability to meet user needs for productive use of electronic information
- Issues involved in migrating
- Costs for hardware and software including acquisition, implementation and ongoing maintenance
- Costs associated with user training
- Professional fees to implement the solutions
- Ability to identify and retain information with long term records value
- Ability to demonstrate chain of custody, record integrity and respond to metadata concerns
- Ongoing support needs required to fully implement the policy

In the evaluation process, an entity should be aware of the differences between enterprise solutions and so-called “point solutions;” technologies focused on solving a specific problem. There are benefits and drawbacks to either approach. Enterprise-wide solutions can be complex and expensive to implement and risk obsolescence over time.

Perhaps the greatest concern is the tendency to focus on the vendor’s view of what are best practices instead of focusing on implementing the entity’s policy. Very few vendors have the perspective necessary to

tailor their enterprise solutions to an individual entity without careful involvement of the purchaser. Similarly, while targeted solutions can be useful tools in an overall strategy, entities should only make such purchases within the context of an overall enterprise-wide strategy, as it can be difficult to integrate different solutions into existing systems.

Finally, an entity should focus on determining the true cost of adding technology to its enterprise. Some solutions may require additional development to properly customize the system to enable it to be integrated with existing disparate systems. As with any substantial purchase, performing due diligence about the vendor and requesting references can assist in making a well-informed decision.

SAMPLE POLICY FEATURES

Policy 1 - Based On Short Default Retention Strategy

Core Policy: Email is retained on an active server only for a short period (e.g., 30 90 days), which is enforced by automatic deletion and, perhaps, limits on mailbox size. The user may avoid the deletion only by taking explicit, affirmative actions like moving the material to dedicated storage on networked files with preassigned retention periods. Litigation holds are applied by users to active email and the automatic deletion feature may be suspended by the entity, as appropriate, for key actors for the period until discovery is complete.

Related Features: Users are expected to discard information, store it locally or on networks or print it out in hard copy and incorporate it into existing file structures subject to records management. Roles and responsibilities are clearly articulated for implementation of the policy, including management of litigation holds.

Pros: This approach may help reduce the rate of growth of additional primary server storage. Selected email with longer-term value is retained by the user, who is best situated to understand the types of records dealt with on a daily basis and is therefore best equipped to make such classifications accurately and effectively.

Cons: The policy may lead to the loss of information needed by the entity in litigation because of the difficulty in accurately identifying the importance of particular information within a short period of time. Users who wish to retain information for longer periods of time may find other methods (like storing files on a local drive or the use of portable storage media) to retain valued email, making subsequent review during discovery more complex.

Legal Assessment: While some courts are uncomfortable with automatic deletion of active email after a short period, no court has found such a process to

be unreasonable where provisions for litigation holds are included and the user has alternative methods of disposition prior to deletion. If discoverable information is not preserved by a user before the copy is eliminated by automatic deletion, but after a preservation obligation has attached, a court will examine whether the use of the automatic deletion feature was “routine” and operated in “good faith,” which is fact specific.

An organization is perfectly free to choose the degree to which it relies upon the discretion of individuals in managing email and applying records schedules; it is not an indication of bad faith to rely on individual user discretion. That said, an organization must provide those employees with adequate training and direction to exercise judgment with respect to the retention and destruction of emails.

Policy 2 - Based On Indefinite Default Retention Strategy

Core Policy: Email is retained on active servers for 60 days and moved automatically to tiered storage and retained indefinitely (or a specified period like 3 or 5 years). The user is permitted to use local archiving or other methods appropriate to his or her work practices. Content management and records management applications are also made available with appropriate search capability for retrieval for litigation or business use.

Related Features: The ability to store information on local hard drives may be restricted to assure centralized storage of all email. A phased implementation might include archiving of legacy email introduced as a second step. Roles and responsibilities, including management of litigation holds, may be specified.

Pros: The approach reduces the amount of data stored on the entity’s email servers, increases assurance of the entity’s ability to access and retrieve information for business or litigation hold purposes, and removes any motivation for users to maintain locally retained information.

Cons: This strategy can significantly increase the amount of stored data that must be searched and reviewed for relevancy, confidentiality, privileges and work product when subject to discovery in litigation. The costs of installation and maintenance of required systems may be large, and the complexity and reliability of some forms of archiving is still an open issue. Finally, entities with a large amount of litigation may find it difficult to find an “open window” in its cycle of repeated litigation holds to effectively dispose of some portion of its ever-growing store of email.

Legal Assessment: No court has held an entity must invest in any particular form of storage technology or otherwise adopt a “save it all” preventative archiving strategy to comply fully with common law obligations to preserve potential evidence for pending or anticipated litigation. However, entities that choose some variation of this approach will have an argument that it is not necessary to pre-

serve less accessible sources that may contain relevant emails (like local hard drives and backup tapes) where it is most likely that such sources contain only duplicate information.

New Employment Arbitration Rules

Many employment arbitrations proceed under the American Arbitration Association ("AAA") rules. Even plans and contract clauses that do not provide for AAA administration use the AAA's rules as the standards for the process. These rules, the Employment Arbitration Rules and Mediation Procedures, have been amended

The amendments address a variety of issues and processes. This memorandum covers the more significant changes.

AUTHORITY OF ARBITRATOR TO DECIDE JURISDICTION

A new Rule 6 gives the arbitrator power to determine jurisdiction and establishes a deadline for challenges to arbitrability. The previous version did not address this question. Rule 6 says:

- a. The arbitrator shall have the power to rule on his or her own jurisdiction, including any objections with respect to the existence, scope or validity of the arbitration agreement.
- b. The arbitrator shall have the power to determine the existence or validity of a contract of which an arbitration clause forms a part. Such an arbitration clause shall be treated as an agreement independent of the other terms of the contract. A decision by the arbitrator that the contract is null and void shall not for that reason alone render invalid the arbitration clause.
- c. A party must object to the jurisdiction of the arbitrator or to the arbitrability of a claim or counterclaim no later than the filing of the answering statement to the claim or counterclaim that gives rise to the objection. The arbitrator may rule on such objections as a preliminary matter or as part of the final award.

PRELIMINARY ISSUES

The new rules specify and expand several details associated with the preliminary stages of arbitration. For example, the old rules did not address the consequences of failing to submit an answer. The revised rules provide that if an answer is not submitted, the claim or counterclaim is deemed denied. Time limits for the submission of answering statements have also been clarified.

In addition, the rules clarify that the AAA will make the initial determination of the city, county, state, territory, and country the hearing will take place in. The rule further provides the arbitrator retains the authority to make the final determination on the issue.

Reflecting common practice, the rules now say arbitration management conferences will be held by telephone unless the parties agree to meet in person.

The AAA also has clarified the provisions about the number of arbitrators. In the past, the AAA might decide three arbitrators would be appropriate in cases with high-dollar demands. The rules now expressly say unless the parties agree to the contrary or the agreement provides otherwise, a single arbitrator will be appointed.

MOTION PRACTICE

The rules now address the question of motions that seek to dispose of a claim or an entire proceeding. Rule 27 says:

The arbitrator may allow the filing of a dispositive motion if the arbitrator determines that the moving party has shown substantial cause that the motion is likely to succeed and dispose of or narrow the issues in the case.

TECHNOLOGY

Several rules have changed to allow modern technology. Rule 28 provides the arbitrator may allow for evidence presentation by web conferencing, internet communication, telephone conferences and means other than in-person. Rule 30 now says that although all evidence must be taken "in the presence" of all of the arbitrators and parties (absent default or waiver), "presence" does not mandate that the parties and arbitrators must be physically present in the same location.

COSTS

The requirements on payment of AAA's administrative fees and arbitrator compensation are now in a separate section. They maintain the distinction between employer-promulgated plans and individually negotiated employment agreements and contracts. In the former, the employer will bear the cost of arbitrator compensation unless the employee elects, post dispute, to pay a portion. AAA will make an administrative determination about the nature of the arbitration agreement. If a party disagrees, they may bring the issue to the arbitrator for a final decision. To streamline the process, the rules provide this determination will be made on documents only, unless the arbitrator deems a hearing is necessary.

AAA & ARBITRATOR IMMUNITY

The old rules said neither the AAA nor the arbitrator would be liable to any party for any act or omission in connection with any arbitration conducted under them. The new rules are more specific by saying:

Parties to an arbitration under these rules shall be deemed to have consented that neither the AAA nor any arbitrator shall be liable to any party in any action for damages or injunctive relief for any act or omission in connection with any arbitration under these rules.

OPTIONAL RULES FOR EMERGENCY MEASURES OF PROTECTION

AAA has adopted new rules that provide for immediate attention to requests for emergency relief. They apply when the parties have entered into a "special agreement" to use the rules or when the arbitration provision specifically adopts them. The Rules create an expedited process for an "emergency arbitrator" to be appointed swiftly and move through the process in a matter of days. The emergency arbitrator, appointed only for emergency relief, is given the authority to issue an interim award determining whether immediate and irreparable damage will result in the absence of emergency relief and whether the party is entitled to the relief sought.

DISCLOSURE

Some of the most extensive changes in the Rules are in rules regarding arbitral disclosure and disqualification. The disclosure rules say:

- a. Any person appointed or to be appointed as an arbitrator shall disclose to the AAA any circumstance likely to give rise to justifiable doubt as to the arbitrator's impartiality or independence, including any bias or any financial or personal interest in the result of the arbitration or any past or present relationship with the parties or their representatives. Such obligation shall remain in effect throughout the arbitration.
- b. Upon receipt of such information from the arbitrator or another source, the AAA shall communicate the information to the parties and, if it deems it appropriate to do so, to the arbitrator and others.
- c. In order to encourage disclosure by arbitrators, disclosure of information pursuant to this Section R-15 is not to be construed as an indication that the arbitrator considers that the disclosed circumstance is likely to affect impartiality or independence.

DISQUALIFICATION OF ARBITRATORS

The process for disqualifying an arbitrator following appointment is now a separate rule, which says:

- a. Any arbitrator shall be impartial and independent and shall perform his or her duties with diligence and in good faith, and shall be subject to disqualification for:

- i. partiality or lack of independence,
 - ii. inability or refusal to perform his or her duties with diligence and in good faith, and
 - iii. any grounds for disqualification provided by applicable law. The parties may agree in writing, however, that arbitrators directly appointed by a party pursuant to Section R-13 shall be non-neutral, in which case such arbitrators need not be impartial or independent and shall not be subject to disqualification for partiality or lack of independence.
- b. Upon objection of a party to the continued service of an arbitrator, or on its own initiative, the AAA shall determine whether the arbitrator should be disqualified under the grounds set out above, and shall inform the parties of its decision, which decision shall be conclusive.

The Hidden Franchise

What do you get when you cross a trademark license, a fee, and elements of control?

Mixed in the right combination, you get a franchise, regardless of what you intend. Many business arrangements that do not look like franchises have been labeled just that. Usually called hidden franchises, they include everything from sales representatives and appliance parts distributors to cafeterias in office buildings.

The franchising we know today started in the 1960's. Continuing into the 1970's, franchises began popping up all over the United States. Not only did the franchise business model take off, so did horror stories about franchisors stealing the life savings of franchisees through fraud, precipitous terminations, and other unfair conduct. Some skeptics saw franchising as little more than a scheme to take advantage of unsophisticated investors. Franchisees took their place among individuals needing special protection by legislatures. California took the lead. Not long after, the federal government stepped in with a law of its own.

Tens of thousands of franchises later, it is a legitimate distribution model. It remains, however, a regulated model through a combination of disclosure and relationship laws at the state and federal levels.

At the federal level, Congress passed a law in 1979 giving the FTC authority over franchising. The FTC Rule identifies a set of disclosures a franchisor must give to a prospective franchisee in a written document with information ranging from the history of the franchisor, the identity of other franchisees and details of any earnings claim or financial performance representations. The FTC Rule does not create a private cause of action. Enforcement is only by the FTC. The unsuspecting franchisor doing business in the 18 states that have enacted laws similar to the FTC Rule is, however, subject to lawsuits by franchisees. These states give franchisees the right to sue their franchisor for damages. Moreover, many states have what are known as "Little FTC Acts" that create a private cause of action for consumers harmed when a defendant breaks a law - acts that some courts have said give franchisees a claim for damages for a violation of the FTC Rule. In addition, potential franchisors are subject to significant damages in the 17 states with franchise relationship laws that punish "franchisors" for terminating franchisees without cause or failing to give proper notice and an opportunity to cure.

DEFINITION OF FRANCHISE

The existence of a franchise relationship is not about labels and it is not about feelings. It does not matter whether the parties call their relationship a "fran-

chise,” a “license,” or a “distributorship,” or whether they “feel” like they are in a franchise relationship, as parties cannot waive protections afforded by the franchise laws. Nor does it typically matter whether the licensee is big or small or otherwise needs the protection of the franchise laws. The existence of a franchise is a matter of definition, pure and simple.

Courts will find that a transaction is a “franchise” if three elements are present: (1) the grant or licensing of a right to use a trademark or trade name; (2) the payment of a “franchise fee” for the use of the mark or name; and (3) some variant of a community of interest, marketing plan, control, or assistance. The definition seems simple enough. For a company trying to avoid the “franchisor” label in the eyes of a court or the FTC, however, the only part of the definition that provides certain protection is the first part - the requirement of a license. As long as a company is not somehow permitting a third party to use a mark or name, it is not offering a “franchise.” As the FTC puts it:

The Commission does not intend to cover package or product franchises in which no mark is involved. If a mark is not necessary to a particular distribution arrangement, the supplier may avoid coverage under the rule by expressly prohibiting the use of its mark by the distributor.

Anytime a company authorizes anyone to use its mark or name and expects to control and be paid for it, that opportunity may well be a franchise, regardless of how it looks, walks, or talks.

MISTAKES CAN BE COSTLY

Navigating the patchwork of federal and state franchise laws is complicated. At the federal level, the FTC Rule applies to franchise opportunities in all 50 states, Washington, D.C., and U.S. territories. A company offering an investment that is a franchise under the FTC Rule must give a prospective franchisee a disclosure document with specific and detailed information about the franchisor and the opportunity. Although a franchisee wronged by a failure to disclose may not have a private right of action, the FTC can bring enforcement proceedings. In states with their own disclosure laws, failing to disclose - or an incomplete or misleading disclosure - allows a franchisee to sue for equitable relief and sometimes damages. In some states, failing to make an accurate disclosure carries the additional risk of exemplary damages, criminal penalties, and fines.

Perhaps most troublesome are the relationship laws adopted in some states. Some of them make it illegal for franchisors to discriminate among franchisees, restrict the ability of franchisors to profit from the sale of goods to franchisees, and regulate the ongoing relationship between franchisor and franchisee. Almost all of these states allow franchisors to terminate only for cause before the

end of the term of the agreement, and then only after providing the franchisee with notice of default and an opportunity to cure. Two states make franchisee agreements “evergreen,” that is, terminable only for cause without regard to their stated term. Thus, a relationship that looks terminable at will may be a franchise that may not be terminated except for cause.

THE THIN LINE

The line between a pure distributorship and a franchise arrangement is often thin, but as many franchisors have learned the hard way, the consequence of crossing it is costly. In one case, Mitsubishi received a rude awakening when the courts decided its distribution system was a franchise. The courts’ analysis hinged on an indirect franchise fee - namely, the payment of over \$500 to Mitsubishi for required service manuals over an eight-year period. The cost was a \$1.525 million jury verdict in favor of the alleged franchisee.

Other courts have followed suit, finding a franchise in general and franchise fee in particular in the most unlikely of places. In another case, the court analyzed whether a license agreement that allowed the plaintiff to sell Ethan Allen-branded products was a franchise. The court said that a mandatory, ongoing advertising fee was a “hidden” or “indirect” franchise fee under Illinois franchise laws.

One court’s franchise fee is sometimes another court’s business expense. The same judge decided that an advertising contribution in one case was an ordinary business expense in another under essentially the same set of facts. In one case the court held that a franchise fee existed where a portion of the plaintiff’s required product purchases was deposited automatically into a mandatory co-op advertising account controlled by the licensor. In another, a dealer’s payments for Yellow Pages advertising, meeting attendance expenses, and advertising co-op contributions were “ordinary business expenses;” not franchise fees given the absence of evidence suggesting the dealer was required to incur these expenses for the right to enter into the business of selling the products.

The Fee

Upfront payments for the right to do business under a particular name or mark and ongoing royalty payments are obvious examples of franchise fees. At the other end of the spectrum, courts have found that ordinary business expenses, optional payments, and wholesale product purchases are not franchise fees. In between these two extremes predictability becomes uncertainty.

Under the FTC Rule, almost any payment might be a franchise fee. The FTC says the “required payment” element of the definition of a franchise is designed “to capture all sources of revenue which the franchisee must pay to the franchisor or its affiliate for the right to associate with the franchisor and market

its goods or services.” A franchise fee can be found in initial franchise fees and those for rent, advertising assistance, required equipment and supplies including those from third parties where the franchisor or its affiliate gets a payment as a result of the purchase including training fees, security deposits, escrow deposits, nonrefundable bookkeeping charges, promotional literature, equipment rental, and continuing royalties on sales.

The FTC Rule and state statutes prescribe certain minimum thresholds and exclude certain types of payments from the definition of a “franchise fee.” The FTC Rule says payments of less than \$500 made to the franchisor or an affiliate before or within six months of opening a business are not a franchise fee. States have a similar exclusion, although the amount varies. Under the FTC Rule and state law, money paid for a reasonable quantity of goods at a bona fide wholesale price purchased from the “franchisor” for resale is exempt from the franchise fee definition.

A transaction that is not a franchise may become one. A fee to continue a relationship, for example, may convert the relationship to a franchise.

THIRD ELEMENT IS A GIVEN

Under the FTC Rule, the third element of a franchise is some sort of “control or assistance” on the part of the franchisor. Alleged franchisors are rarely successful in claiming that they do not somehow “control” the alleged franchisee. At its simplest, any control by a franchisor over a franchisee and any assistance to a franchisee will qualify as “control” as long as the FTC believes it is “significant.” It does not take much to reach any measurable level of significance. Training programs, operation manuals, and establishing methods of operation all meet the test.

Some states require a “community of interest” between franchisor and franchisee. Courts applying the laws of these states rarely fail to find a community of interest in even the most basic forms of product and service distribution relationship. In some states, a community of interest exists where both the alleged franchisor and franchisee profit from the sale of a product or service, which is always the case where a royalty is based on sales. Others require the presence of a “marketing plan or system” before labeling a relationship a franchise. California courts have held that oral or implied and optional or suggested plans and systems meet the test. Careful companies do not count on the third element to save them from being called a franchisor.

SAFE HARBORS

The FTC Rule and most states exclude a number of relationships from their definition of a franchise for disclosure purposes. For example, a business op-

portunity that will constitute merely a part of a company's existing business falls within the "fractional franchise" safe harbor. The FTC Rule, however, allows the exemption only when the franchisee has more than two years prior management experience in the business represented by the franchise and where the parties anticipate that sales under the franchise will represent no more than 20 percent of the dollar volume of the franchisee's projected gross sales. Some states exclude sales to purchasers with a high net worth or a high income, and several states exempt sales by large franchisors from the registration requirement. Further, isolated sales are exempted by the FTC and a few states.

THE BOTTOM LINE

The bottom line is that the creation of a franchise relationship and the duties of disclosure, opportunity to cure, termination only for cause, etc., is not a question of magic language. Whenever a deal involves a trademark license, a fee, and elements of control or a community of interest, it may be a franchise under applicable law. Given this risk, the careful distributor of a product or service under a mark or name should follow the franchise laws, including a disclosure document or an offering circular. A licensor still wanting to avoid the burden of a disclosure document and the risk of liability under various franchise laws must exercise great caution.

Internet Job Application Recordkeeping

Recruiting and hiring is increasingly sophisticated and complex, especially with Internet and other technology use. The improved communications means greater ease in soliciting applicants and responding to openings. These advances call for more precision in the way recruiting is handled. One of the biggest problems is dealing with the increase in inquiries about jobs and applications.

Most employers are covered by federal employment laws. This mandates keeping appropriate records as a result of all employment relationships for a specific period of time. While some statutes do not mandate retaining specific types of records, most require retaining specific information. Having records on hand is important to defend suits by employees or applicants. These records extend to when a person is being considered for a job. The increase in inquiries and applications generated by electronic recruiting has created large record-keeping responsibility for employers.

Beside having good documentation, there are records employers are legally required to keep. For example, many large employers must track and document job applicants and employees annually to report group identification to the EEOC and the OFCCP. Federal contractors subject to Executive Order 11246 and other rules require copies of affirmative action plans be retained. Both of these make it necessary for employers with government contracts to track information about job applicants. They must establish ways of distinguishing job applicants from casual inquirers so they can report to the OFCCP and determine whether there is a disparate impact on protected groups.

WHO IS A JOB APPLICANT?

Record-keeping obligations begin before actual hires. One of the more difficult issues employers face in complying with record-keeping requirements is the question of who is a job applicant. Answering that has never been easy. It is more complicated using the Internet and other new technologies for recruitment. In 2005 the OFCCP issued rules on the definition of “Internet job applicant” for the data retention and record-keeping obligations of federal contractors.

An individual used to be considered an applicant if he or she filed a formal application or indicated in an informal way a specific intention to be considered for a job. Someone who casually appeared at an office or a work site to make an informal inquiry was not considered an applicant. An “applicant” under the

Uniform Guidelines on Employee Selection Procedures (Uniform Guidelines) has typically been a person who indicated an interest in being considered for hiring, promotion, or other employment opportunities. While not problem free, employers had concrete ways of knowing whether a person was actually applying for a job or just making an inquiry; and they had fewer inquiries and applications to record and maintain.

The Uniform Guidelines serve two purposes. They address certain record-keeping issues by describing the evidence employers should have available to determine whether their employment selection procedures have a disparate impact on protected groups. They also detail methods for validating tests and selection procedures found to have a disparate impact. Such a practice or standard is unlawful if it is not job-related and consistent with business necessity.

The Uniform Guidelines say employers should maintain records or other information that will disclose the impact which its tests and other selection procedures have upon employment opportunities of persons by identifiable race, sex, or ethnic group. It provides for employer self-analysis for disparate impact based on those records or other information. Enforcing agencies may use those records or other information to investigate disparate impact charges or litigate cases.

Specifically, the Uniform Guidelines provide for the maintenance of records or other information on applicants. The 2005 revision to the 1979 guidance says that Internet or related electronic data technologies includes:

- E-mail;
- Internal and third-party resume databases;
- Job banks;
- Electronic scanning technology;
- Applicant tracking systems/applicant service providers; and
- Applicant screeners.

A person using those sources will be an applicant if the following criteria have all been met.

- An expression of interest in employment is made by the individual through the Internet or related electronic data technologies;
- The employer considers the individual for employment for a particular position;
- The expression of interest indicates that the individual possesses the basic qualifications for the position.

- At no point in the selection process prior to receiving an offer of employment does the individual remove herself from further consideration or otherwise indicate no further interest in the position.

The final rule says that if an employer considers any expressions of interest made through the Internet, then all expressions of interest, regardless of means and manner, meet the definition of Internet job applicant. If an employer accepts both Internet applications and traditional applications, all of the applicants, Internet and traditional, are Internet job applicants for the rule.

The phrase “considers the individual for employment in a particular position” means the employer assesses the substantive information provided with respect to any qualifications involved with a particular position. The employer does not have to consider all who have expressed interest. An employer may implement policies to limit the number of expressions of interest actually considered as long as the policies are applied uniformly in a manner facially neutral and without producing a disparate impact. Specifically, the rule says employers may establish procedures whereby they do not consider expressions of interest if they were not submitted according to established procedures; or not submitted for a particular position. Also, an employer may use data management techniques to limit the number of expressions of interest considered, like random sampling or absolute number limits.

“Basic qualifications” means those qualifications the employer advertises as required for an individual to be considered for the position. If the position is not advertised, the basic qualifications are those the employer establishes and makes a record of before considering any expressions of interest for that position. Basic qualifications must be:

- Noncomparative;
- Objective and not dependent on the employer’s subjective judgment; and
- Relevant to performing the particular job and enable the employer to accomplish business-related goals.

What qualifies as removing oneself from further consideration or otherwise indicating no further interest in the position means:

- An express statement of no further interest by the individual;
- A passive demonstration of disinterest by the individual (repeated non-responsiveness to inquiries from the employer concerning interest in the position);
- A lack of interest inferred from information contained in the expression of interest made by the individual (like salary requirements, work type and lo-

cation preferences) as long as these inferences are uniformly and consistently applied.

RECORD RETENTION REQUIREMENTS

Records of expressions of interest by individuals made through the Internet must be maintained if the employer considered the individuals for the particular position. Record-keeping, with respect to expressions of interest through internal resume databases, must consist of:

- A record of each resume added to the database;
- A record of the date each resume was added to the database;
- The position for which each search of the database was made;
- The substantive search criteria used; and
- The date of the search.

When an external resume database is used, the employer must keep records of the following:

- The position for which each search was made;
- The substantive search criteria;
- The date of the search; and
- The resumes of job seekers who met the basic qualifications for the position who were considered by the employer regardless of whether the individual qualified as an Internet applicant.

Records of the race, gender, and ethnicity of each job applicant must be kept where possible. There is no set point in the selection process where this information must be gathered, nor is there a set procedure to acquire the information. The OFCCP says self-identification is the preferred method, but visual observation may be used if the applicant will not self-identify.

CONCLUSION

The final rule modifies OFCCP job applicant record-keeping requirements to address problems encountered by the use of Internet and electronic data technologies in the job applicant recruiting and hiring process. Although the final rule, as discussed above, imposes a number of new, additional requirements on contractors/employers, its stated intent is to address those record-keeping and data collection problems.

Maintaining Your Corporate Veil

Limiting shareholder liability has always been a primary purpose of having a corporation. Not surprisingly, maintaining the “corporate veil” has always been on the checklist of lawyers advising any multi-business company. With the rash of products liability and consumer class actions, coupled with large jury verdicts, businesses today must be extra careful to protect the corporate veil. Companies need to manage risks carefully, identify potential exposures and plan for the possible claims that the liabilities of a corporation may be imputed to related corporations or their owners. This is generally called “derivative risk”.

Derivative risk exposure is of particular concern for both foreign-based entities with investments in the US and diversified US businesses. This memorandum looks at six steps multi-business companies may use to reduce the chance that the separate identity and limited liability of a corporation will be disregarded.

ISOLATING LIABILITIES AMONG SEPARATE ENTITIES

A corporate owner, whether an individual or another company, is not normally liable for the corporation’s debts. The law permits creating separate entities to, among other things, isolate liabilities among them. Courts recognize a public policy of encouraging investments and affording limited liability to shareholders. There are exceptions. When a court decides that a corporation is an “alter ego” or “mere instrumentality” of its shareholders, the court may “pierce” or disregard the corporate veil to prevent injustice or fraud, or do justice or equity. Despite whole books on the subject, deciding whether a corporation is an alter ego or mere instrumentality of its shareholders is essentially based on the circumstances. There are steps that serve to mitigate the risk of veil piercing.

Maintaining the corporate veil is often in tension with effective management models and tax strategies. Companies need a measured, practical approach that considers the following as ways to demonstrate a subsidiary’s separateness. None of these alone would instantly defeat a veil-piercing claim, and some may not be practical for some businesses. They are a reasonable starting point.

Observing corporate formalities.

Following corporate formalities is widely acknowledged as a factor on whether to maintain a corporate veil. They vary from state to state, but include annual shareholders’ and directors’ meetings; regular election of officers and directors; maintaining corporate record books including all meeting minutes; and managing the subsidiary consistent with its charter and bylaws. Observing these for-

malities costs almost nothing in terms of management or tax concerns. Good corporate and financial records are also the basis for upholding the business judgment rule.

Separation of funds and accounts.

Whatever formalities are observed, any claim that a parent and a subsidiary are legally separate entities is not likely to win when they do not separately account for their finances. When corporate veils have been pierced, there has typically been abuse of a subsidiary's accounting and financial functions. This does not mean a parent and subsidiary may not achieve economies of scale through cash management strategies. In those situations companies must keep separate accounts and books, record monetary transfers and properly document transactions.

Subsidiary operations will commonly be reflected on the parent's financial statements. It is important that each subsidiary's financial condition be consolidated through the accounting records of its direct parent or parents; not "reported up" to a functional business unit or group or unincorporated parent business divisions. It is better to observe formalities even when there is functional management of the overall enterprise.

Adequate capitalization.

A subsidiary should be capitalized at a level consistent with the level of risk associated with its business operations. Courts routinely focus on capital levels when considering piercing a corporate veil, though adequate capital is an imprecise concept. A subsidiary should have enough capital to operate without frequent, random and unplanned capital infusions. If a parent repeatedly funds a subsidiary when liabilities arise in the ordinary course, there is a real risk it will also be required to fund the subsidiary under extraordinary situations.

The parent should not siphon funds away from the subsidiary through excessive dividends, even though tax considerations may suggest otherwise. The test is whether the dividend is in the best interest of the subsidiary; not the parent. The subsidiary should regularly review its capital position and its board of directors should make an annual decision, (properly recorded in the annual meeting minutes) of the adequacy of working capital and the subsidiary's ability to pay dividends.

Directors and officers; corporate control.

The management of any corporation is vested in its board of directors - not shareholders. Each subsidiary should have its own board of directors, which appoints the officers of that subsidiary. The subsidiary board should supervise the officers and the performance of the subsidiary.

In reality, the parent to protect its significant investment appropriately exercises substantial control. In the public company context, this is needed to satisfy its fiduciary obligations to its own shareholders. Complete domination of the subsidiary creates a risk a court will decide the parent is liable for the subsidiary's debts. There is a legitimate concern that too much authority in a subsidiary's board can be a threat to the investment. These interests can be balanced by having representatives from the corporate parent on the subsidiary board. Indeed alternative is generally lawful and preferred to the common practice of periodic inquiries from a representative of the parent that often leads to fodder for plaintiffs' lawyers and regulators.

Intercompany transactions.

Intercompany transactions are critical for multi-business companies to achieve synergies, and should be made on terms that allow businesses to take advantage of these benefits. These transactions can create exposure to a veil-piercing claim when they bear the marks of control and influence that do not reflect arms-length interaction. These transactions should be fully documented, and, under certain circumstances, approved by the boards of directors of all companies in the transaction. These transactions should be on commercially reasonable terms, though not necessarily on terms normally extended to an outsider.

Managing perceptions.

How a subsidiary corporation holds itself out to the public can be important. "Subsidiary" implies a separate legal entity. Words like "division," "department," "unit," and "group" imply unincorporated businesses that are part of the same legal entity (and protected by limited liability). A subsidiary that makes excessive use of the parent's name, other marks or goodwill may be creating the impression the two companies are single. Some public companies say in public filings that the subsidiaries are separate legal entities, subject to decentralized management, and governed by corporate control structures applicable to the subsidiaries' jurisdiction of organization.

KEY ISSUE

In most cases, the important question is not whether a veil-piercing claim will win but whether the other side can make a viable claim as leverage. The more a parent and subsidiary behave like a single entity, the more likely a claim to pierce the corporate veil will withstand initial review.

Open Source Code

There are four “classic” open-source licenses. These are the GNU Public License (GPL), the Limited GNU Public License (LGPL), the Berkeley System Distribution and the Massachusetts Institute of Technology (MIT) license. With the open-source release of the Netscape Web browser in 1998, the Mozilla Public License is also widely used. Many other open-source licenses have been created. There are over 60 open-source licenses approved by OSI.

Of all the open-source licenses, the GPL license is the most prevalent. Most components of the popular GNU/Linux system, including the Linux kernel itself and most system utilities and applications, are licensed under the GPL. Leaders in the open-source community urge developers to use the GPL. A 2002 estimate was that 90% of all open-source software was licensed under the GPL.

Many companies find open-source software components provide high quality at low cost compared to commercial alternatives. This is an incentive to use open-source software as a building block for proprietary products.

However, under GPL, a licensee may be required to release its own source code if it distributes or publishes a derivative work based on a GPL-licensed program. Setting aside when a work is considered “distributed” and “derived” under the GPL, companies may find themselves in the position of having to either release their proprietary source code or lose permission to distribute, copy or modify the modified software.

Licensees can choose to release their source code and comply with the GPL. However, choosing this route must understand the GPL requires derivative works to be licensed “as a whole.” This may include not only the main source code, but also interface definition files and related scripts. It is often not possible to simply carve out selected proprietary portions of the source code.

SEPARATING OUT PROGRAMS

One way around the requirement is to put proprietary code into identifiable sections of a work that is not derived from the Open-Source program, as contemplated by § 2 of the GPL. These separate sections must reasonably be considered independent and separate works in themselves. They must be truly distinct from other GPL-licensed works, and not part of a whole which is a work based on the program.

What this means is not entirely clear. On one extreme, simply aggregating programs is permitted under GPL. On the other extreme, a proprietary program that is separate but relies entirely on a GPL-licensed program to function is likely considered part of a whole work based on the GPL-licensed program, requiring the source code to be released.

Between these extremes are many shades of gray, where two programs may communicate, interoperate or function in parallel and where GPL offers little guidance on the duty to release. One risk of using GPL or other open-source licensed code as a building block for proprietary products is the uncertainty regarding precisely when the duty to release code is imposed.

Many companies would rather not release source code for fear of giving up trade secret protection. Making matters worse, GPL prohibits distribution of a derivative work in the event patent or other royalties are exacted. While copyright protection is available, it is generally limited to nonfunctional aspects. This leaves developers between a rock and a hard place. Releasing source code could mean giving away proprietary information. On the other hand, licensees choosing not to release source code but distributing their software could be liable for copyright infringement.

The GNU project urges donors of any substantial amount of code to assign rights to the Free Software Foundation (FSF), in part to facilitate enforcement actions. FSF operates a compliance lab to monitor GPL violations and take enforcement action where necessary. FSF has not been hesitant to enter negotiations with heavyweights over suspected GPL violations. One case has already been filed. In Germany, a group unrelated to FSF, but having the same goal, has received at least two injunctions against companies that have failed to release source code. These enforcement efforts show that the duty to release source code should not be taken lightly.

DUTY TO RELEASE SOURCE CODE

Given the repercussions of releasing source code, it is important to know when this duty is imposed. There are two aspects to this duty - distribution and derivative works. Unfortunately, GPL does not use consistent or well-defined language for either.

GPL requires releasing source code when licensees distribute or publish any work that in whole or in part contains or is derived from the program or any part thereof. In connection with distribution, GPL uses the additional language “third parties” to qualify when a work might be distributed. Redistribute is used in the context of how a license is automatically granted to successive licensees.

In connection with the derivative work aspect, GPL imports the definition of a derivative work from copyright law, but then uses the phrase “work based on the Program” more expansively, suggesting the two terms are not coextensive.

Adding confusion, the legal term “collective work” is also used in GPL, but its definition under the Copyright Act as a “work constituting separate and inde-

pendent works in themselves” was not imported into GPL. This suggests a broader duty to release code, not confined simply to derivative works. Likewise, the Copyright Act defined term “distribution” has not been explicitly imported into GPL. This raises the issue of whether “distribution” under GPL is coextensive with “distribution” in copyright law. The absence of clear definitions and consistent terms makes it difficult for licensees to know their precise responsibilities to when it comes to releasing code.

For example, a licensee may make minor proprietary modifications to a GPL-licensed program, and pass it on without the accompanying source code for testing. Is the modified program a “derivative work”? If so, is it also a “work based on the Program”? Should we focus on whether the licensee’s act is a “distribution,” or the status of the recipient as a “third party”? The GPL FAQ’s discuss these issues, but its interpretation is aimed at resolving practical rather than legal issues, and is not binding on courts.

RISK OF INFRINGING COPYRIGHTS

Another risk of using open-source software is that it will be found to infringe on existing copyrights. This risk does not come from GPL itself, but from the possibility of unpoliced submission of proprietary code into open-source projects. Although a risk when using any software product, it is more of a risk in open-source projects, where the code is open to public inspection. This risk can be reduced by educating developers about the legal standard of substantial similarity in the context of copyright law, which focuses on the abstraction-filtration-comparison test in *Computer Associates International Inc. v. Altai Inc.* Under this test, determining substantial similarity involves; abstraction of the plaintiff’s program; filtering out any nonprotectible elements; and comparison between the remaining core of protectible expression and the defendant’s work.

GNU Developer Guidelines urge programmers who have vague recollections of the internals of a Unix program they wish to imitate, to organize their work internally along different lines. Merely using a different internal organization is a problem because of court rulings which hold that copyright law may protect the structure, sequence and organization of the source code. Another issue is that a programmer’s familiarity with proprietary code could create a finding of subconscious copying. An open-source developer could infringe the copyright of a familiar proprietary product by inadvertently imitating its code, as contemplated by the GNU Developer Guidelines, even if not deliberately copying its structure, sequence or organization.

Donors of code into GNU and other open-source projects are normally required to represent they have ownership rights and obtain necessary disclaimers from employers. However, those representations are not a warranty, indemnification against claims of infringement, or other legally binding protection against fu-

ture claims by any party, other than the donor's employer. Thus, despite the freedom to distribute, copy and modify code, licensees of open-source software should be aware that their own use is only permissible to the extent the original licensor holds a valid copyright.

There are other legal risks. For example there are certain legal issues in combining nonfree libraries with GPL-covered software. There is also the issue of how to reconcile incompatible open-source license provisions, a particular concern in complex releases that may contain dozens of different open-source components.

In addition to indemnification provisions, proprietary software licenses frequently provide warranties against defects in media, viruses, worms, Trojan Horses and backdoors. In contrast, GPL software is "as is," without warranties. In addition, maintenance and support, also common in proprietary licenses, are often lacking in GPL.

Trademark & Trade Secret Record Retention

We are frequently asked for recordkeeping recommendations on these two subjects. Here are some suggestions.

TRADEMARKS

A trademark is a word, phrase, symbol or design, or combination of words, phrases, symbols, or designs, which identifies and distinguishes the source of the goods or services of one party from those of another.

Trademark rights arise from either (1) the actual use of the mark, or (2) filing an application to register a mark in the U.S. Patent and Trademark Office (PTO) stating the applicant has a bona fide intention to use the mark in interstate commerce.

Registration

Federal registration is not required to establish rights in or to use a mark. It can secure benefits beyond the rights acquired by just using a mark. Filing an application is constructive notice of use, which prevents a junior user from acquiring any right to use the mark after the filing date. Once issued, the registration is constructive notice which prevents a junior user from acquiring rights to the mark and confines the rights of a senior, unregistered user to the territory that user occupied at the time of the registration. Other advantages of federal registration include presumptions of validity, ownership, and the exclusive right to use the mark, increased ability to block infringing imports, and possible eligibility for the mark to attain incontestable status.

Trademark rights can last indefinitely if the owner continues to use the mark. A trademark may be registered for ten years with ten-year renewal terms. Companies will want to maintain records identifying exactly when a trademark renewal date is approaching so as not to lose valuable rights.

A trademark registration must be maintained or it will be canceled. Between the fifth and sixth year after an initial registration, the registrant must file a continued-use affidavit to keep the trademark active. A registrant is also required to file a continued-use affidavit in the year before the end of every ten-year period after the registration date. The affidavit must set out those goods or services recited in the registration on or in connection with which the mark is in use in commerce and must be accompanied by specimens or facsimiles showing current use of the mark. If the mark is not in use, then the affidavit must show that it is due to special circumstances that excuse non-use and is not due to any intention to abandon the mark. There is a six-month grace pe-

riod after the end of the applicable period within which a trademark owner can still file its § 8 affidavit, along with a surcharge.

Section 9 of the Lanham Act requires a registrant to file a renewal application every ten years. The renewal application must be filed sometime within the year before expiration of the ten years. There is also a six-month grace period in which the PTO will still accept a renewal application.

A mark can attain incontestable status if the registrant files an affidavit with the PTO within the sixth year of use stating the mark has been continuously used on the goods or services listed in the registration for five consecutive years and is still in use. A registration that is incontestable is conclusive evidence of validity, ownership, and the exclusive right to use the mark in commerce.

Finally, a registrant should give notice that the mark is registered with the PTO by displaying the mark with the words "Registered in the U.S. Patent and Trademark Office" or "Reg. U.S. Pat. & Tm. Off." or with the ® mark. If the registrant does not give notice, the registrant cannot receive profits or damages in an infringement suit.

Trademark Infringement

In a trademark enforcement action, a company will have to show it diligently protected its trademark from migrating into the public domain. Conducting trademark searches and documenting them is essential to a defense.

If the company becomes aware of possible infringement, it must take steps to protect the trademark. Initially, this may be a cease-and-desist letter, and may, eventually, proceed to litigation. All records pertaining to the steps the company has taken to protect its trademark will be important to any litigation.

TRADE SECRETS

Another area of intellectual property where detailed record keeping is essential is trade secrets. A company will want to identify its trade secrets. A host of different things can be considered trade secrets; customer lists, advertising plans, software, designs, competitive strategies, pricing, supply sources, salary structures, recruiting practices, particular ways of doing business, or manufacturing methods. Once the company has identified its trade secrets, the key is to then protect them so they do not lose their trade secret status.

There is no provision under federal law for registration of trade secrets. Trade secrets are protected under many state laws and under the Economic Espionage Act of 1996, a federal law that criminalizes and establishes considerable fines for the theft of trade secrets.

Most trade secret litigation will boil down to whether the company can produce records showing it has adequately protected the particular trade secret. A company must have procedures in place to protect both its trade secrets and other companies' trade secrets. For example, during discussions with inventors, negotiations with a potential candidate for acquisition, or even in correspondence with a potential supplier or customer, a trade secret may be divulged. There is usually an implied or express obligation on the company not to use or appropriate confidential information or trade secrets except for the purpose for which the information was disclosed. A company may also receive outside idea submissions from third parties. If the company accepts such an idea and then develops the same idea, it could become involved in trade secret litigation.

An example is a case where a snowmobile manufacturer could not show, through its records, that it had been independently working on an electronic fuel-injection engine similar to one another company had developed and disclosed information about to the manufacturer during licensing negotiations. After the negotiations broke down, it began to manufacture its own fuel-injected engines for snowmobiles. Because it could not produce evidence showing it had independently developed the fuel-injected engine, the jury decided it had misappropriated the trade secrets it acquired in the licensing negotiations. The jury ordered \$45.6 million for trade secret misappropriation.

This highlights the importance of records like:

1. The identification of the research personnel working on a particular project, and the dates, time frames, and at least some discussion of the details of the subject matter of the technology being developed;
2. How the company plans to use the technology; and
3. Research and development the company is subcontracting out.

Creating A Trade Secrets Records Retention Program

Some of the initial considerations in creating a records retention program to keep track of trade secrets include:

1. Who should maintain this kind of information?
2. Where is research and development taking place? (It could occur in a research and development laboratory, the shop floor, the MIS department, or even the advertising and marketing departments.)
3. Which employees have access to the trade secrets?
4. How often should the information be updated?
5. In what form should the records be kept?

Employment-related records. Suppose a company hires an engineer from a competing company and that engineer is working on essentially the same technology with the new company as with the prior one. Without an enforceable noncompetition agreement, the law says:

- The engineer could not take trade secret information, including specific trade secret knowledge the engineer had in his or her head, or actual documents or samples, from the previous employer.
- On the other hand, general information and general knowledge the engineer developed in his career, including the job with the competitor, is something the engineer can use in future work for anyone.

The dilemma comes where the engineer develops something really useful competitive with products of the prior employer. Did the engineer improperly use trade secrets or confidential information from his previous job for his new employer? This is a heavily factual issue.

Another complicating factor is whether the company intended the engineer use the secrets of the previous company in developing its products. It is one thing when an engineer is just careless with confidential information. It is quite another when a company has an intent or policy to hire engineers from a competitor to acquire its competitor's trade secrets.

The general consensus is that a company should get a statement that the person hired has not taken any documents relating to trade secret or confidential information from the prior employer. This includes computer disks, programs, and digital information e-mailed from one computer to another. The wording should be broad enough to cover documents of all types. It may also be helpful to get a statement as to exactly what the engineer was working on at the prior company and, if appropriate, create documentation showing the engineer is not using that knowledge or data in the current job.

If a company maintains detailed records of the products or services it is developing with an accounting of the progress being made on them, it will make it easier to prove these products or services, if they compete with those of an employee's prior employer, were developed independently. This should be adequate to meet allegations that the development and production of the products or services in question were not the result of trade secret misappropriation.

Companies hiring new employees who have had access to another company's trade secrets should sign confidentiality agreements. Companies also must keep records of the noncompetition agreements employees have signed. Records of entrance and exit interviews explaining what trade secrets are and reinforcing what trade secrets must be kept confidential after the employee leaves

should be conducted and documented. If possible, an employer should learn who an employee's new employer is and notify that employer what trade secrets the employee may be privy to. Documentation of those letters should also be appropriately retained. Contracts with outside sales personnel and vendors should also include provisions for trade secret protection, if applicable.

Records of security measures. Records of the security measures the corporation has in place to protect trade secrets should also be available. This can include everything from properly documented security at the company's facility to logs that track visitors to the facility, to records of surveillance.

Internet and e-mail. A company should have procedures in place to monitor whether its trade secrets are disclosed by e-mail, on the company Web site, or over the Internet. A case involving Ford underscores how important it is, especially in the age of the Internet, for corporations to protect their trade secrets.

Ford got a temporary restraining order for various copyright and trademark law violations after the defendant published internal Ford documents and used the Ford trademark on its Web site. The defendant was a Ford MUSTANG fan who decided to start his own Web site. Ford, interested in getting more "consumer" input in designing the next generation of MUSTANG issued him a media pass and let him get close to Ford employees at various company events. The fan began receiving documents from anonymous disgruntled employees critical of the MUSTANG. He published these on his Web site.

Although the documents were not marked proprietary, Ford said some of the documents were highly confidential, including one about its emissions strategy. The court refused to issue a permanent injunction. The court decided the fan's First Amendment rights outweighed Ford's interest in protecting its proprietary information. The court prohibited the fan from disseminating additional documents from Ford employees and warned against soliciting new documents.

Companies can be retained that will monitor the Internet for possible infringement.

Employee ideas and outside idea submissions. A doctrine called the "shop rights" doctrine essentially says if an employee developed an idea within the scope of employment, on the employer's time, and using the employer's equipment, the idea will generally belong to the employer. Companies should have formal procedures specifying these employer rights in writing upon an employee's idea submission. The company should also have written agreements for accepting ideas from outside.

Requests for information. A company should keep records of requests for potential trade secret information made under laws like the Freedom of Information Act or the Occupational Safety and Health Act's Hazard Communication Rule. Under these laws, certain information is subject to disclosure to anyone

who requests it; however, trade secret information is generally exempted from disclosure requests.

Trade Secrets Records Retention Checklist

A common issue in trade secret litigation is whether the information is really a secret. For example, a customer list that is

1. Stamped "trade secret confidential information";
2. Made available to employees only on a need-to-know basis;
3. Always accompanied by a document signed by the employee which says no copies will be made;
4. To be returned when the need for it ceases; and
5. Not to be disclosed to anyone else, should qualify as a trade secret.

On the other hand, that same customer list simply passed around indiscriminately in the company with no safeguards will probably not be a trade secret.

Here are common problems companies face in their effort to identify, maintain, and protect trade secret and confidential information.

- Does the company have a written "inventory" specifically listing the company's trade secrets?

A central issue in trade secret disputes and litigation is whether the company actually took appropriate steps to safeguard trade secret information or merely claimed something was trade secret after a former employee began using it with a competitor. Maintaining a current written inventory goes a long way in helping in this type of dispute.

The inventory itself is not confidential. It should be disclosed to appropriate employees. A customer list could be distributed among employees with a notation to the effect that the customer list contains trade secrets and is to be treated as confidential information. That would hopefully cause employees to treat it properly and would be helpful in addressing a former employee who leaves and solicits customers for a new employer. It would be difficult for the employee to argue that the identity of the customers was never mentioned as a trade secret or confidential information.

- What records does the company have which support that the information was really treated as a trade secret?

Assume an employee leaves taking trade secret information to a competitor and the competitor begins to use it. You ask a lawyer about your remedies,

and the lawyer asks what evidence you have to support the fact that the information was actually kept as a trade secret.

There are many ways to support your trade secret claim. There are no specific rules. All too often a company realizes it has no procedures to safeguard its trade secrets. This creates a loss of negotiation leverage. In a lawsuit, it may mean losing the case. Some things it might help to maintain so that they can be used in this situation include:

- Records of training sessions about trade secrets, including the general substance of the training, people attending and sessions;
 - Memos circulated to staff which indicate the trade secret nature of the information;
 - Policies and procedures which say how the information should be kept together with records on how they were actually enforced;
 - Relevant documents stamped with a legend (it is NOT good to stamp everything with this legend); and
 - Records of the use of safeguards like passwords and controlled access.
- Does the company have records that establish each employee has signed a nondisclosure or confidentiality agreement?

Many companies require such agreements as part of the hiring process. With transfers, acquisitions, and divestitures, it is possible these records will be impossible to locate when needed. An audit that examines how the company keeps these records would be helpful.

- Does the company's records retention program take into account confidentiality agreements entered into with customers or suppliers?

For valid business reasons, companies often enter into agreements with others that involve disclosing trade secrets. Records of these agreements can be used to contest the coming allegation that this information was handed out without a requirement that it be kept secret.

Shareholder Liability for Copyright Infringement

An area where shareholders are not shielded from liability for the acts of a corporation is copyright infringement under the Copyright Act. While it is well settled that shareholders can be liable under the Act, the test for determining shareholder liability is unsettled.

This memorandum outlines the circumstances under which a shareholder can be held liable for the acts of copyright infringement committed by a corporation.

TEST FOR VICARIOUS LIABILITY

The Second Circuit Court of Appeals, in a case called Shapiro, first established the two-part vicarious liability test for determining when third parties could be held liable under the Act. The court held that when the right and ability to supervise combine with an obvious and direct financial interest in exploiting copyrighted materials even without actual knowledge that a copyright infringement is happening, the purposes of the law might be best served by imposing liability on the beneficiary of the infringement.

That decision cited no provision of the Act as a basis for holding that vicarious liability can be imposed on a third party. In fact the Act does not contain any provision on contributory liability or vicarious liability. Regardless, the Supreme Court and other courts have followed Shapiro in imposing vicarious liability on a third party if that party maintained the right and ability to control the infringing conduct and had a direct and obvious financial interest in infringing the copyrighted material.

Right & Ability to Control

A litigant seeking to reach a shareholder for a copyright infringement committed by a corporation first must show the shareholder had the right and ability to supervise the conduct of the infringing corporation. The Shapiro case put emphasis on a party's right to police the conduct of the primary infringer.

The "power to police" as the Court put it, has proven difficult to apply. Some courts hold that the actual exercise of control is not required and all that is needed to establish liability is the legal right and ability to control and supervise the infringing conduct. Other federal courts put emphasis on whether the alleged vicarious infringer in fact exercised actual control and supervision of the infringing conduct.

Direct Financial Interest

A plaintiff trying to hold a shareholder vicariously liable for the copyright infringement of a corporation also must show the shareholder had an obvious and direct financial interest in exploiting the copyrighted work allegedly infringed. Courts have not developed a bright-line test for deciding when a party has a sufficiently direct financial interest in the infringing activity to warrant the imposition of liability. Most courts say stock ownership in the infringing corporation establishes a sufficiently direct financial interest in the infringing activity. Some courts even gloss over the issue and instantly conclude that the financial interest of certain parties is obvious. Other courts require evidence of a direct financial benefit.

VICARIOUS LIABILITY IN OTHER CONTEXTS

The vicarious liability test applied in copyright infringement claims is different than the vicarious liability test applied to other cases. The distinctive difference is there is no requirement that the right to control extend to the manner and means of performance. This stems from the policy goals underlying copyright.

Modern decisions, when explaining policy justifications for vicarious liability commonly refer to risk allocation. When an individual profits from an enterprise in which identifiable types of losses are expected to occur, they hold it is fair and reasonable to put responsibility for those losses on the person who profits, even if that person makes arrangements for others to do the acts that cause the losses.

The law of vicarious liability treats expected losses as a cost of doing business. The enterprise and the person profiting from it are better able than either the innocent injured plaintiff or the other person whose act caused the loss to distribute the costs and shift them to others who have profited from the enterprise. Putting responsibility for the loss on the enterprise has the added benefit of creating incentive for the enterprise to police its operations carefully to avoid unnecessary losses.

LIABILITY OF SHAREHOLDERS

Because vicarious liability for copyright infringement allows copyright owners to reach parties ordinarily shielded from liability, they frequently sue shareholders for a corporation's alleged infringement. These suits seek to hold shareholders jointly and severally liable for infringements by the corporation. This is particularly useful when the corporation is not able to satisfy a judgment on the claim. The legal test for deciding whether a shareholder may be liable for the copyright infringement by a corporation will vary depending on whether the shareholder is an individual or a corporation.

Individuals as Shareholders

Very few cases put vicarious liability on an individual shareholder not an officer or director of the corporation. Courts imposing liability on an individual shareholder almost always emphasize their status as a shareholder only for the financial interest prong of the test; finding the required control through the individual's service as an officer or director of the corporation.

One case held an individual vicariously liable for copyright infringement on the ground that as president of a corporation, he supervised the infringing conduct and, as a fifty-percent shareholder, financially benefited from the infringements. The court said that despite his claim that he had no right to supervise the retailers, he did supervise them by writing letters instructing them on what uses of the copiers to permit.

Another case held the president and sole shareholder liable where he personally approved an infringing sale through a broker. He also approved the price to be charged for the copies. While the record did not reveal whether the president and the corporation actually made money from the transaction, an inference was made that both anticipated profits from the sale.

While other federal appellate courts have not addressed this issue squarely, a consensus has emerged among district courts that an individual's status as a shareholder determines only the financial interest prong of the Shapiro test and cannot by itself satisfy the supervision and control element of the vicarious liability test.

Corporations as Shareholders

The leading case in this area ruled that a parent corporation couldn't be liable for infringement by a subsidiary unless there is a substantial and continuing connection between the two with respect to the infringement. The following facts showed a substantial and continuing connection existed with respect to the infringement: (1) the subsidiary was wholly-owned; (2) the parent corporation's legal counsel responded to the allegations of infringement; (3) the parent actually hired the employee who created the infringing works; and (4) the employee who created the infringing works maintained an office at the parent corporation. On these facts, the parent could be held vicariously liable for the copyright infringement committed by the subsidiary.

Most district courts have followed this standard.

UNSETTLED QUESTIONS

Federal courts have not resolved the question of whether an individual shareholder not serving as an officer or director of a corporation may be held vicariously liable for the copyright infringement of a corporation. Those courts following a legal control standard of liability might impose vicarious liability

against a majority shareholder because the shareholder has the theoretical right to control the conduct of the infringing corporation. Those following an actual control standard of liability likely would require evidence of an individual shareholder's involvement in the day-to-day operation before imposing vicarious liability.

Succession Planning Benefits & Risk Management

INTRODUCTION

Rapid change means you often need to replace key management staff on short notice. There is increased pressure to remain competitive and an increasingly competitive market for skilled individuals. All these prompt you to effect succession plans.

Succession planning identifies and helps groom candidates for future openings in key positions due to lost leadership, new markets or new environments.

Succession planning is best when it is part of and tied to a strategic plan. Once you identify long-term goals and objectives, you forecast staffing needs consistent with these goals and objectives. You must ask yourself: who will replace executives, managers, professionals and other key employees, and where will those replacements come from? Integrated strategic and succession planning helps you recognize that future executives may need substantially different qualifications, characteristics and skills than today's leaders.

OVERVIEW

The aim of succession planning is to plan personnel moves so candidates for key positions are known before actual need. This allows opportunities for mentoring and development to improve readiness to succeed in specific positions. It also provides concrete information for decision making to minimize poor choices or the adverse impact of unplanned vacancies on continuity of management.

The three basic goals of succession planning are to (1) identify critical positions in the organization; (2) forecast future vacancies in those positions; and (3) identify managers and other employees who would potentially fit those vacancies.

Succession planning can also help you:

- Grow future executives instead of having to recruit externally;
- Manage diversity through systematic development of women and minorities;
- Shorten the learning curve for future managers;
- Increase employee loyalty and commitment;
- Shift from job progression to job expansion;

- Move toward being a learning organization;
- Recognize increasingly demanding and escalating competencies are required; and
- Recognize new roles are needed to manage and revitalize new business, business units, front-line positions or growing product lines.

Different Approaches

Traditional succession planning involves CEOs and other top executives identifying their own replacements in a secret process where no open discussion occurs about candidates selected. It involves manual systems. Human resources staff may or may not be involved, and HR processes like performance appraisal systems and management development typically are not included. Replacement candidates usually are not informed about their selection. Assessment from peers, customers or subordinates is not part of the process. This approach does not emphasize personal, career or team development.

A more integrative approach involves both succession planning and succession development. It incorporates system processes and automated tracking systems to assure objectivity and consistency. It lays the foundation on which managers can make decisions on succession at executive and other key employee levels. It is future-oriented and consistent with strategic planning. It is flexible, responsive to change and linked to other human resources planning activities.

SUCCESS AND FAILURE

Keys to Success

Top management commitment. Top management must be both committed and willing to commit necessary resources. This means a solid business case must be made for the process and plan.

Strategic vision of necessary future skills. To know what skills you will need in the future, you must examine workplace trends, projections for graduates in critical fields, etc. It is also necessary to speak with company leaders about where the business is heading and the skills employees will need in the future.

Understanding the existing workforce. You need to evaluate how many of your key employees will be eligible for retirement or may leave in upcoming years, and how many employees may be ready, willing and able to move into vacated positions. You must understand where you may face technical skills gaps and whether you can identify existing staff with the knowledge or potential to fill them. You also must understand where this workforce information resides and how to make it accessible.

Open mind about employees and skills. Succession planning sometimes focuses too much on obvious top performers - those employees who are easily and clearly identified as “up and comers.” Stopping with these employees limits your potential. Hidden talents can be in less visible workers. Some of these employees may self-identify; others have to be encouraged. A succession plan should involve educating existing staff so they understand where the gaps will be and are in a better position to step forward and express interest in performing a particular role or function.

Solid plan and strong organization. Succession planning is a quantitative, analytical exercise that requires good organization skills, attention to detail and ability to project into the future. A good succession plan must be designed to capture necessary information, store it, allow for its manipulation to generate reports and develop “what if” scenarios, and to be modified as the work force changes or projected organizational needs change.

Accountability. Some managers are threatened when asked to participate in identifying future leaders. The succession plan has to belong to the whole organization and not just the HR department. Senior management must hold all managers accountable for identifying talent among their staff members, even to the extent that compensation and promotion are to some extent tied to success in identifying and developing future talent.

Good training and development program. If you decide you need employees skilled in a particular area, but do not have this talent, you have two choices: recruit externally or develop opportunities for interested staff with identified potential to learn necessary skills. In-house training, special project assignments and outside coursework are necessary to avoid over-reliance on external recruitment.

On-going attention. It is easy to overlook succession planning in favor of more immediate needs. Continued ownership by top management is necessary to keep it a priority.

Common Problems

Underestimating the talent in the organization. Many organizations overlook the level of talent they have. Consider how many of your employees might be considered experts by the competition and whether you want to risk losing them.

Narrow-minded thinking. It is critical to not overlook employees who perhaps are thought to be too old, too young, too rough around the edges or too different.

Too much focus on hard skills. Soft skills like emotional intelligence often are more important in determining success than more traditional hard skills or technical abilities. Consider organizational culture and teamwork needs beside technical requirements.

Not offering appropriate training and development opportunities. You should not leave employees to fend for themselves in building skills. Training is part of the program and appropriate resources must be available.

Not holding managers accountable for succession planning. You should not let managers become an obstacle to succession planning because of insecurities and biases.

Considering only upward succession. Lateral succession may be a need in many organizations. Many companies have dual career paths. Just because hierarchies and organizations get smaller at the top does not mean the ability of employees to grow and develop should be limited. Employees can grow by exposure in different areas even if they are not advancing up the hierarchy.

Developing a one-size-fits-all program. Generic leadership development programs are not effective as a form of succession planning. Individual succession plans based on specific organizational needs, specific individual skills and training work better.

OTHER KEY POINTS

Formal planning is preferable. No formal plan means you cannot proactively have leaders develop the skills they need to assume the next level of responsibility because you will not know what roles to move them into and cannot communicate to leaders what their potential future is in the organization. This gives the appearance you either don't care or aren't strategic enough to know.

Some succession planning programs are over-designed with too many forms, too many criteria, too much training and a high time demand on managers. The result is a perception of the plan as bureaucracy. Some companies avoid this by integrating succession planning into the yearly performance review process so managers are evaluating current year performance and future years' potential succession likelihood at the same time.

Older succession plans were based on identifying "high-potential" pools. A downside of that phraseology and approach is the implication that people not in the pool don't have high potential. Look at succession planning as the means to identify candidates from a wide range of leadership levels and accelerate their growth by broader experience and exposure. In other words, the system is not just about finding high-potential candidates, but also about finding and broadening the job experience of unsung heroes to maximize their contributions to the organization.

A modern way to view the potential of employees is to focus on strengths in four areas: (1) leadership promise (the motivation to lead and ability to bring out the best in people while being authentic in relationships with others); (2) personal development orientation (being receptive to feedback and having broad learning ability); (3) balance of values and results (individual fits the culture and has passion for results); and (4) ability to master complexity (individual is adaptable, thinks conceptually and can deal with and address business ambiguities).

Should succession planning be secret?

The question of whether or not to tell high-performing workers that they have been identified in the succession planning process is controversial.

An advantage to secrecy is that it allows you to keep your options open. As business conditions change, a manager or the company may feel that a different kind of person is needed to fill a key vacancy. A disadvantage to secrecy is that high-performers may leave the organization because they don't see a future for themselves.

In contrast, when employees are told they have been identified, they are more likely to stay because they see a possible future. Disadvantages to sharing this kind of information are that high performers may stop performing because they believe a promotion is "in the bag" or that managers may inadvertently commit to what the employee believes is a binding obligation to promote.

The potential drawbacks of communicating succession planning have prompted many companies to keep the process secret. High performing companies usually are open about the process. Most such companies are committed to a positive working environment for all employees and don't want a two-class system to emerge. They tend to have as a fundamental premise that everyone is treated well and everyone will know where they stand regarding performance. Companies that are best at succession planning tell high potentials what their status does not mean. It does not mean a promotion to a high-level job next year, it is not a permanent designation, and it probably means an increased burden to prove the perceived potential.

LEGAL ISSUES

The key risk with succession planning is that it can be or be perceived as a system that pre-selects for key positions based on age.

It is a reality that many, when considering staff for promotion to higher-level positions, will favor younger employees. Business reasons often exist to support this.

If a succession plan is not properly written, if training for management about how it works is not properly carried out, or if misstatements are made about how the system operates or its effects, then the line between a planning system for key positions and a selection system that is closed to older employees may blur and evidence may be created that the system is a tool of age discrimination.

The Supreme Court has ruled that disparate impact claims can be brought under the Age Discrimination in Employment Act (“ADEA”), but the scope of such claims is narrower than under Title VII in two ways: (1) an employee is required to identify a “specific” employment practice responsible for any statistical disparity applies, and (2) based on the “reasonable factors other than age” provision in the ADEA, “a reasonableness inquiry” is used in place of the Title VII “business necessity” test in age disparate impact cases. This helps planning succession plans.

A succession plan should (i) be written and put in place in a way that negates any claim that it is the specific basis for any age disparate results in promotion, and (ii) the succession plan should articulate the reasonable, non-age-related justification for its existence and substance.

Succession planning programs, if not carefully created and implemented, can appear to be a pre-selection device that violates other EEO laws – those proscribing race, sex or other forms of discrimination. For example, the plan may appear to exclude persons of color, to effect a glass ceiling for women or to favor a particular nationality or race.

The potential for problems increase if the management succession plan is secret, if the ages of individuals are identified and pictures are included (revealing race, color or nationality) and the succession plan then is subject to discovery in a lawsuit.

Where companies are not secret about the plan and tell promising candidates about their selection as a retention strategy, carefully consider how to do that in a legally defensible way.

This requires coaching from HR and counsel to ensure that legally binding promises are not made to mollify an otherwise outstanding performer to keep that employee.

A succession plan should never become a promise of job security or a guarantee of a promotion; it should only indicate a worker’s potential has been noted, which then has certain effects with respect to maximizing skills and abilities.

Steps to take:

- The line between manpower planning and promotion decisions must be distinct. The plan language should support this.

- Assume all succession planning materials will end up in court.
- Including personal and family information, photographs, and other EEO information is not useful. The essential information should be an assessment of needed abilities and skills, leadership capability, emotional intelligence or whatever other traits and attributes an individual is deemed to have and then, to the extent needed, a delineation of training and development opportunities the individual may need and how all of this relates to the potential to fill particular positions that may open at future times.
- Management succession documents should not be the primary document used in key promotion situations.
- Monitor the process and plan to make sure neither excludes protected groups and does not include discriminatory statements.