



Anticipating and Responding to Litigation

A Legal and Practical Guide to Managing Data in Preparation of and in
Response to Litigation

3	Introduction
4	Knowing When the Duty to Preserve Arises <ul style="list-style-type: none">i. Levels of Culpability and Appropriate Sanctionsii. Burden-Shifting
8	Roadmap to Complying with Preservation Obligations <ul style="list-style-type: none">i. Create a Legal Hold Response Teamii. Know Where Your Data Livesiii. Archive Your Dataiv. Institute a Defensible Document Retention Policyv. Implement the Legal Holdvi. Notify Custodians of the Legal Holdvii. Release the Legal Hold
11	References

This document does not provide legal or other professional advice and should not be relied upon as anything other than a starting point for research and information.

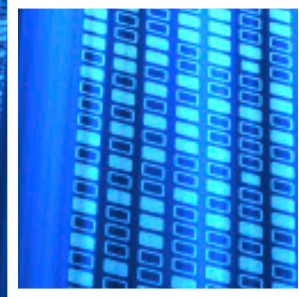
Copyright © 2010 Kroll Ontrack Inc. All Rights Reserved.

Kroll Ontrack, Ontrack and other Kroll Ontrack brand and product names referred to herein are trademarks or registered trademarks of Kroll Ontrack Inc. and/or its parent company, Kroll Inc., in the United States and/or other countries.

Introduction

In today's digital world, organizations must manage data in a manner that mitigates legal risk and possible sanctions for failure to safeguard and preserve potentially relevant electronically stored information (ESI). According to Kroll Ontrack's Year in Review report, approximately 40 percent of all e-discovery cases in 2009 involved claims for sanctions against parties that allegedly failed to comply with discovery obligations. Of the cases involving a claim for sanctions, 66.67 percent addressed an alleged failure to properly preserve ESI. The growing body of statutory and common law regarding electronic discovery instructs litigants that the best defense against sanctions is to take proactive measures to fully comply with future discovery obligations. Ignorance is no longer tolerated and there is decreasing judicial tolerance for preservation mistakes, oversights or intentional destruction.

Prior to litigation, corporations can help avoid spoliation by thoughtfully managing data in a manner that contemplates a swift and effective response. Preparing to respond to legal inquiries requires knowing when the duty to preserve arises; in other words, understanding facts or events that "trigger" a responsibility to identify and preserve potentially relevant information. But even before that, proper preparation requires knowing where and how data is stored, along with installing a process to regularly dispose of unnecessary data, retaining only the data that is needed for business continuity purposes (ex. disaster recovery), regulatory matters (ex. financial data) and/or legal matters. Once a corporation has notice of an actual or anticipated legal matter, a defensible response includes issuing a written legal hold notice to relevant custodians and identifying other sources of potentially relevant data to ensure that data is properly preserved until the legal matter is no longer anticipated or has concluded.



Knowing When the Duty to Preserve Arises

Despite the growing body of case law on the topic, knowing when the duty to preserve arises is a key issue that continues to plague corporations. Once a lawsuit, audit or investigation begins, organizations are considered to have been provided actual notice and are subject to a duty to preserve potentially relevant paper documents and ESI. This is a clear, well-established obligation. (For a recent example, in the Southern District of New York, United States Magistrate Judge James C. Francis, IV found that the duty to preserve arose no later than the lawsuit's filing.ⁱ) However, more often than not the duty to preserve arises prior to the commencement of litigation or an investigation. Unfortunately, the Federal Rules of Civil Procedure provide little guidance as to when a party's duty to preserve is triggered. Thus, litigants must rely on the facts and instructive case law to determine the proper course of action in these modern digital times.

Following *Zubulake v. UBS Warburg LLC*, a landmark series of discovery decisions published from 2003-2004, it is well established that the duty to preserve arises upon reasonable anticipation of litigation. “[O]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.”ⁱⁱ The “reasonable anticipation” rule is well-settled. However, the subjective nature of the standard often leads to confusion and uncertainty when determining what constitutes reasonable anticipation. As such, it is the duty of individual entities to discern when preservation is required and to issue written legal hold notices in response.

A “trigger event” is an event that creates notice of foreseeable litigation and activates an organization’s duty to preserve paper documents and ESI that may be relevant to the underlying matter. Trigger events come in many different forms and are highly dependent upon the facts and circumstances of individual cases. Although there are limited bright-line rules that require parties to preserve relevant ESI (notice of a civil filing, for example), examination of relevant case law offers great insight into other “trigger” events that provide clear notice of pending, potential, or anticipated investigations or litigation.

Generally, pre-litigation correspondence qualifies as notice of potential litigation or investigations and triggers a duty to preserve relevant information. In a case from the District of Maryland, the duty to preserve

arose when a plaintiff sent a letter informing the defendant that he had consulted attorneys regarding the matter.ⁱⁱⁱ The Western District of Kentucky has held that notice of litigation was established after a phone call from the plaintiff and the filing of a complaint.^{iv} Additional courts have determined pre-litigation trigger events to include: threatened legal action in writing,^v conversations with supervisors and management,^{vi} filing claims with administrative agencies,^{vii} and letters from opposing counsel prior to litigation.^{viii}

In the context of litigation, a plaintiff's duty to preserve is more frequently triggered prior to the commencement of litigation because plaintiffs are in control of the litigation's timing. In *Innis Arden Golf Club v. Pitney Bowes, Inc.*, the court held that the plaintiff's duty to preserve arose upon the retention of counsel even

Corporations can help avoid data spoliation by thoughtfully managing data in a manner that contemplates a swift and effective litigation response.

though the parties were still unknown.^{ix} Similarly, in *Indemnity Insurance Company of North America v. Liberty Corp.*, the seriousness of injuries and losses, attempts to document damage via photographs, and the immediate retention of experts and counsel to assess and report damages, were all factors determined by the court to trigger the plaintiff's duty to preserve.^x

As demonstrated by these sample cases above (which by no means present an exhaustive list of possibilities), it is no surprise that parties are confused as to when the duty to preserve arises. And, to strengthen defensibility, parties should take detailed notes of the preservation protocol that was followed, which includes when the hold was issued, what details were included in the hold, to whom the hold was issued and the efforts taken to monitor compliance.

Tip: Prudent corporations quickly implement written legal holds if litigation appears to be on the horizon.

Failure to Preserve and Resulting Sanctions

It is often difficult to discern bright-line distinctions between acceptable and unacceptable conduct in the context of preservation and discovery.^{xi} "Whether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done or not done was proportional to that case and consistent with clearly established applicable standards."^{xii} Inherent in the determination of whether sanctions are warranted and appropriate remedies are the

culpability of the spoliating party, the level of prejudice sustained by the party seeking discovery and whether counsel took affirmative steps to monitor whether its client was complying with its duty to preserve.^{xiii}

Levels of Culpability and Appropriate Sanctions

In the context of data spoliation after the duty to preserve has attached, the spoliating party's culpability can range from inadvertent loss, to mere negligence, to intentional destruction of evidence or willful misconduct. As a general rule, higher degrees of culpability warrant the imposition of increasingly severe sanctions. Ultimately, sanction determinations are heavily dependent upon the facts and circumstances of each individual case; therefore, the basic rules provide practitioners and litigants with little affirmative guidance. However, a recent opinion issued by District Judge Shira Scheindlin of the Southern District of New York, has drawn clear connections between culpability and conduct. In this case, *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*,^{xiv} Judge Scheindlin addresses specific findings of culpability and the sliding scale of corresponding sanctions that may arise when a party fails to fulfill its discovery obligations.

With regard to culpability, Judge Scheindlin defined the standards of negligence, gross negligence and willful misconduct. According to Judge Scheindlin, negligent behavior falls below the standard of acceptable conduct. In the discovery context, acceptable conduct is determined by "what a party must do to meet its obligation to participate meaningfully and fairly in the discovery phase of judicial proceeding."^{xv} A party who fails to meet this acceptable conduct standard has acted negligently regardless of whether the actions resulted "from a pure heart and an empty head."^{xvi} Behaviors constituting simple negligence include failing to obtain records from all employees, to take all appropriate measures to preserve ESI, to assess the accuracy and validity of selected search terms, or to collect evidence.

Gross negligence is a standard greater than simple negligence and is a failure to exercise the same level of care a careless person would employ. Accordingly, Judge Scheindlin defines the following as gross negligence: the failure to issue a written legal hold, identify the key players and ensure that their electronic and paper records are preserved, cease the deletion of e-mail or to preserve the records of former employees that are in a party's possession, custody or control, and preserve backup tapes when

A "trigger event" is an event that creates notice of "reasonably foreseeable" litigation or investigation and activates an organization's duty to preserve paper documents and ESI.

Knowing When the Duty to Preserve Arises

they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.

Willful, wanton or reckless misconduct includes an intentional act, indifferent to the consequences, which “make[s] it highly probable that harm would follow.”^{xvii} Judge Scheindlin cites the intentional destruction of relevant ESI or paper documents as examples of willful misconduct, especially if the conduct occurred after the final relevant *Zubulake* opinion was issued in July 2004. The actions described as grossly negligent (discussed above) may be deemed willful if the party’s actions are intentional.

Judge Scheindlin notes that these behaviors are not meant to establish a definitive list, but are rather meant to serve as examples of discovery failures and culpability levels. *Pension Committee* holds that sanctions may be imposed for spoliation of electronic data that is the result of negligent and grossly negligent conduct – not just willful misconduct.^{xviii} According to Judge Scheindlin, the least harsh, yet most adequate sanction available should be imposed, ranging from sanctions such as cost-shifting and fines to evidence preclusion and default judgment. While Judge Scheindlin states that the terminating or default judgment sanction should be imposed only in the most egregious discovery misconduct. According to her opinion, adverse inference instructions are an appropriate remedy for gross negligence or willful misconduct.

The *Pension Committee* decision has grabbed hold of the legal

community. Although the specific definitions of unacceptable conduct and relationship levels of culpability provided in *Pension Committee* are not meant to establish a definitive list of bad behavior that will result in sanctions, commentators widely believe this opinion raises the bar of acceptable conduct for litigants.

Another recent opinion, issued by Judge Lee Rosenthal of the Southern District of Texas, “limits the applicability of the *Pension Committee* approach.”^{xix} In this case, *Rimkus Consulting Group, Inc. v. Cammarata*, Judge Rosenthal addresses preservation and spoliation issues in the context of intentional actions. In this matter (which arose out of a dispute over the terms of an employment agreement) the defendants claimed they routinely deleted e-mails as part of their business practice. However, the court determined the defendants intentionally lost, altered and deleted e-mails and found it appropriate to send the case back to a jury with a permissive adverse inference instruction.

The *Rimkus* opinion drew several distinctions between it and *Pension Committee*, particularly in regard to the circuit differences concerning the issue of culpability. According to Judge Rosenthal, the sanction of adverse inference instruction based on a finding of gross negligence found in *Pension Committee* is at odds with the requirements in other jurisdictions. In the Fifth Circuit, severe sanctions, including default judgment, striking pleadings or adverse inference instructions, may not be imposed unless there is evidence of bad faith or the intentional destruction of evidence.^{xx} Furthermore, Judge Rosenthal notes that the Eleventh

Circuit has ruled that bad faith is required for an adverse inference instruction and that the Seventh, Eighth, Tenth and D.C. Circuits appear to require the same.^{xxi}

Burden-Shifting

Regardless of which approach is followed in determining appropriate sanctions for the spoliation of evidence, the specific type of sanction also directly correlates to which party, the innocent or spoliator, bears the burden of establishing the relevance of missing evidence. Judge Scheindlin specifically addressed this issue in the *Pension Committee* case.

Judge Scheindlin explored the burdens associated with the loss of documents, analyzing who is responsible for demonstrating the relevance and resulting prejudice of the lost evidence, and related the burden of proof question to the severity of the sanctions at issue. For less severe sanctions, such as an award of costs and fees, the court’s inquiry focused on the loss of evidence, and whether it was relevant or resulted in prejudice. Essentially, the innocent party must prove three elements: the spoliating party had control over the evidence and an obligation to preserve when the evidence was destroyed, the spoliating party acted with a culpable state of mind, and that the missing evidence is relevant.

On the other hand, when more severe sanctions are considered, such as dismissal or an adverse inference, the inquiry of the court focuses on behavior, in addition to the relevance and prejudice caused by the unavailability of evidence. Moreover, if a spoliating party is found to have acted in a

grossly negligent manner or in bad faith, relevance and prejudice may be presumed. However, Judge Scheindlin notes that this presumption is not required and is always rebuttable.

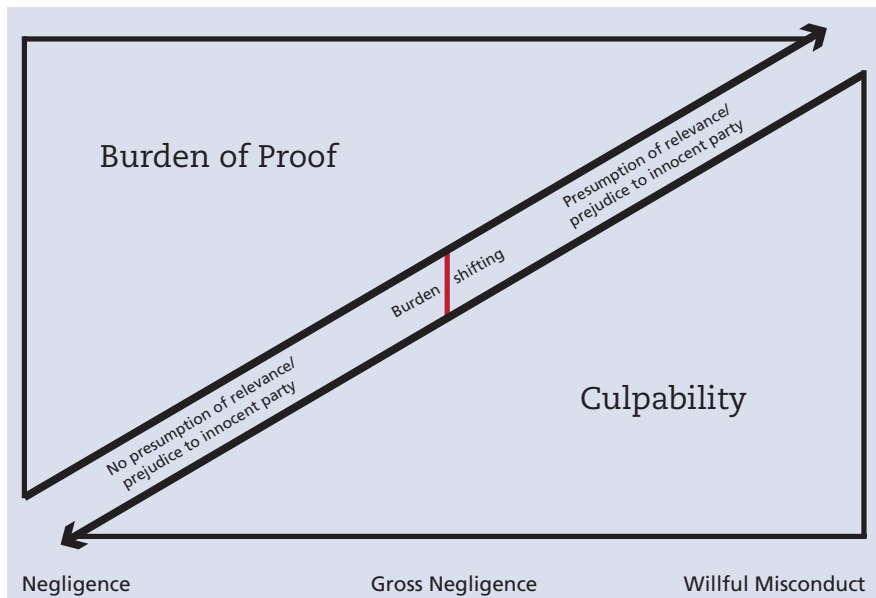
In summary of her discussion on this issue, Judge Scheindlin set forth a burden-shifting test as follows: if a spoliating party's conduct is egregious enough to justify the imposition of a presumption of relevance and prejudice or if the conduct warrants permitting the jury to make a presumption, the burden shifts to the spoliating party to rebut the presumption. If the spoliating party demonstrates no prejudice occurs, then no jury instructions would be warranted, although the possibility for lesser sanctions remains open.

Judge Scheindlin notes the burden-shifting test seems to place a substantial burden on innocent parties since it requires an innocent party to demonstrate the relevance of evidence that it may never review due to the opposing party's failure to preserve. Judge Scheindlin acknowledges this seems unfair, but states that "the party seeking relief has some obligation to make a showing of relevance and prejudice, lest litigation become a 'gotcha'

game rather than a full and fair opportunity to air the merits of a dispute."^{xxii} An automatic presumption of relevance and prejudice would motivate parties to find errors and capitalize on mistakes, which the Judge felt "would not be a good thing."^{xxiii}

In another point of distinction, Judge Rosenthal, author of the Rimkus opinion, limits the application of the Pension Committee principles in relation to adverse inference instructions. Judge Rosenthal notes that case law in the Fifth Circuit demonstrates that a showing of relevance regarding the spoliating evidence is required in order to issue an adverse inference instruction.^{xxiv}

Both the *Pension Committee* and *Rimkus* decisions provide useful insight into the types of behaviors deemed unacceptable in the world of electronic discovery. The messages of these cases are clear. As Judge Scheindlin reiterated, although perfection is not required, parties must take the necessary steps to properly preserve relevant records for collection, review and production.



Pension Committee Approach:

When seeking severe sanctions, as the level of culpability increases, the innocent party's burden to prove the relevancy of the spoliating documents to the underlying case (and resulting prejudice) decreases. The burden shifts to the spoliating party to rebut a presumption of relevance and prejudice if the behavior was grossly negligent or willful.

A Roadmap to Complying with Preservation Obligations

Legal Hold Response Team

During an investigation or litigation, corporations must be well-versed on the available technology to identify and preserve potentially relevant information and comply with discovery obligations. However, before technology is considered, corporations must give serious thought to the team of individuals involved in the administration and maintenance of the tools and the processes around implementing, monitoring and releasing legal holds. As such, corporations should enlist a multidisciplinary team of individuals to help drive and support the legal hold process to ensure that it efficiently and promptly complies with its legal duties.

The formation of the team and selection of its members should begin with broadly and clearly-communicated support from the highest levels of top management to best ensure the team's ability to effectuate change and comply with legal duties. And, all functional areas of the organization should be considered when forming a response team. The response team should know where company data resides, how it is maintained, how it can be accessed and when it is destroyed. Comprehensive response teams will include employees from various corporate departments and disciplines, including but not limited to information technology, legal, business line managers, corporate records management, human resources, risk management and administration.

While the formation of an interdepartmental response team is essential to the successful implementation, execution and monitoring of legal holds, these teams are not without challenges. It is likely that response team members will have diverse levels of legal or technical knowledge as well as different priorities and perspectives. As such, conflicts are not only normal, but almost unavoidable when the response team is initially formed.

Tip: In order to minimize conflicts, teams should be formed early (prior to the need to respond to litigation or investigation) and the goals and objectives of the team clearly communicated.

Know Where your Data Lives

An organization must know where its data is stored before it can effectively manage that data in a manner that contemplates and prepares for future litigation. Many organizations catalog and monitor data through creating and maintaining an application inventory and data map. Together, an application inventory and data map help corporations and outside counsel quickly identify relevant data sources and custodians that are key to an investigation or litigation, and prevents the need to search for information throughout every storage system within the organization's IT environment.

Functional Areas to Consider When Creating Your Litigation Response Team:

- Corporate Counsel
- IT
- Records Managers
- Risk
- Compliance
- Human Resource
- Business Group Leaders
- Outside Experts

Once the application inventory and data map is in place, it must be routinely updated to stay current with the constant evolution of an organization's technology environment. The updates should complement technology asset management processes, storage planning, information security assessments and other processes that impact the IT environment. When applications or systems are retired, information should be included as to where the final set of data is kept and what process will be required to restore if necessary. Maintaining the current and comprehensive nature of this information will save time, effort and cost down the road. This will also strengthen defensibility arguments if the opposing party moves for spoliation sanctions in the event data is inadvertently lost or otherwise does not get preserved.

Tip: An application inventory and data map should include:

- a record of operating systems and application software
- back-up rotation procedures and schedules
- contact information for department point persons

Archive Your Data

After determining where data lives, it should be ingested, de-duped and indexed within an archive platform. Most of the relevant content in an organization is contained within e-mails and attachments, loose files (such as

word processing, spreadsheets and presentations) on network shares and collaboration/document management platforms (such as Microsoft® Sharepoint®). In addition to the network, key sources of ESI may be found on employee workstations/laptops/PCs and external hard drives. Many archiving platforms can ingest the data on PCs and external hard drives when these devices are connected to the company network.

Tip: An archiving solution will not only ensure that business continuity objectives are being met, but help legal, IT, records managers and compliance teams preserve, manage, locate and produce relevant ESI in a legal or investigatory proceeding.

Institute a Defensible Document Retention Policy

The implementation of an archiving system is an integral part of a repeatable, defensible document retention policy. A defensible retention policy will classify records per a records retention schedule that dictates how long each record classification should be kept, and contain citations of applicable document retention regulations in order to ensure compliance with regulations and industry standards. Once an organization has comprehensively determined the universe of records to be maintained, proper maintenance and necessary document destruction policies may be determined.

Tip: Create a data retention policy that incorporates emerging technologies such as instant messaging, unified messaging and social media. As more organizations use these technologies to conduct business, IT, records managers and corporate counsel will need to address and define the use and storage of this type of data.

Implement the Legal Hold

Incorporating legal hold technology as part of an overarching data archiving system will allow users to search throughout an IT enterprise to identify and immediately preserve potentially relevant ESI, reducing risks of spoliation. Data that is found to be not relevant to investigation, regulatory matter or litigation can also be easily released, decreasing the volume of data stores for later analysis, processing and review.

Practically speaking, archives apply a legal hold on content from a search collection, effectively suspending the document retention and disposal. Conversely, legal hold tools that operate outside of an archiving platform collect copies of the data, have no control over primary repositories of data, and bare the risk of not being identified and copied, inadvertent alteration, and over-collection. Legal holds within archives maintain control of the data for as long as the investigation or matter is ongoing. Sophisticated archiving tools allow for granular release of legal holds

A Roadmap to Complying with Preservation Obligations

for messages and files determined to be not relevant. Messages and files released from a legal hold will resume its record-class retention schedule.

Tip: It is typical practice to collect a larger set of data and “lock it down” with a legal hold as early as possible. Then, the collection can be later filtered and reviewed with far less risk of data spoliation.

Notify Custodians of the Legal Hold

As soon as the subject, date range and custodians are determined, the organization is required to issue a written legal hold to data custodians regarding the anticipated litigation or investigation. Data custodians include authors and users of data, but also data “stewards” such as IT administrators, department heads and even third-party vendors that may hold, store and otherwise exercise control over potentially relevant data. Typically, legal hold notifications are sent by e-mail, requesting that employees keep all data that meets the notice criteria. Follow-up messages are sent, often requiring employees to provide a list of content and data location(s) that meet the parameters of the legal hold notice.

Most legal hold protocols require that an employee reply to the hold notification with 1) an acknowledgement of receipt and 2) an agreement to comply.

Once the target universe of data has been collected and

contained within an archive, an authorized user, typically within the general counsel’s team, will winnow the data set down to only potentially relevant content before proceeding to the next stage of the discovery process. The authorized user will typically accomplish this through searching the archive against criteria such as keywords, custodians and date ranges. Typical filters include removing “junk mail” and out of office bounce-back messages. The archive will log the initial search parameters, results and all further filtering steps taken. It will also provide a history, status and progress of each search collection, legal hold, filters, categorizations and granular release for the supervisor of the legal team to monitor. Once the authorized user is satisfied with a search collection, a legal hold is applied and messages and files may be categorized as relevant, privileged and confidential. The data set may then be exported for early case assessment or document review.

Release the Legal Hold

At the conclusion of an investigation or legal matter, the legal hold may be released for all of the content within the hold. However, other investigations or matters might also have applied legal holds to some of the content. A capable archiving system will support concurrent matters, ensuring that any data being held for multiple matters is not released when only one of the matters is settled. As such, an archiving system will not allow the scheduled retention and disposal policy to resume until all legal holds have been released on the message or file.

References

- i Green v. McClendon, 2009 WL 2496275 (S.D.N.Y. Aug. 13, 2009).
- ii Zubulake IV, 220 F.R.D. at 218.
- iii Goodman v. Praxair Servs., Inc., 2009 WL 1955805 (D. Md. July 7, 2009).
- iv KCH Servs., Inc. v. Vanaire, Inc., 2009 WL 2216601 (W.D. Ky. July 22, 2009).
- v PML N. Am., LLC v. Hartford Underwriters Ins. Co., 2006 WL 3759914 (E.D. Mich. 2006)
- vi Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372 (D.Conn. 2007)
- vii Zubulake IV, 220 F.R.D. at 218.
- viii Optowave Co. v. Nikitin, 2006 WL 3231422 (M.D. Fla. Nov. 7, 2006)ix European Convention on Human Rights of 1950, Article 8; See also Dorothy Heisenberg, Negotiating Privacy: The European Union, The United States and Personal Data Protection (2005).
- ix Innis Arden Golf Club v. Pitney Bowes, Inc., 257 F.R.D. 334, 340 (D.Conn. 2009)
- x Indemnity Ins. Co. of N. Am. v. Liberty Corp., 1998 WL 363834 at *4 (S.D.N.Y. June 29, 1998).
- xi Rimkus Consulting Group v. Cammarata, 2010 WL 645253 (S.D.Tex. Feb.19, 2010) at *5.
- xii Id.
- xiii Id., Zubulake III, 229 F.R.D 422,
- xiv Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).
- xv Id. at *3.
- xvi Id.
- xvii Id.
- xviii Id.
- xix Rimkus Consulting Group, 2010 WL 645253 at *6.
- xx Id. at *5.
- xxi Id. at *5.
- xxii Pension Comm., 2010 WL 184312 at *5.
- xxiii Id.
- xxiv Rimkus Consulting Group, 2010 WL 645253 at *6.





9023 Columbine Road
Eden Prairie, MN 55347
800 347 6105
www.krollontrack.com

Copyright © 2010 Kroll Ontrack Inc.
All Rights Reserved.

All other brands and product names are
trademarks or registered trademarks of
their respective owners.