



A CommVault White Paper: Addressing e-Discovery and Legal Hold Requirements with CommVault

**CommVault Corporate Headquarters
2 Crescent Place
Oceanport, New Jersey 07757-0900 USA
Telephone: 888.746.3849 or 732.870.4000**

Addressing e-Discovery and Legal Hold Requirements with CommVault

Table of Contents

Executive Summary	1
What is Legal Hold?	1
Why is Legal Hold Important? A Case Study	2
Case Summary: Zubulake vs. UBS Warburg, LLC	2
Responding to Increased Legal Risk – What Data to Keep?	3
The Federal Rules of Civil Procedure	4
FRCP Rule 37	6
When Does an Organization Have to Put Information on Hold?	6
What Needs to Be Put on Legal Hold?	7
Litigation Response Planning	8
CommVault’s Solution Suite	10
Legal Hold Process with CommVault Suite	11
Conclusion	15

Addressing e-Discovery and Legal Hold Requirements with CommVault

Executive Summary

Recent amendments to the Federal Rules of Civil Procedure (FRCP) have put a spotlight on how organizations respond to electronic discovery requests. While the amendments provide some clarification, they lack specificity on how to avoid the costs and risks associated with not living up to the expectations of the courts. This has left organizations grappling with how to best prepare for litigation.

One area where organizations are looking for help is around litigation response planning and how to effectively place information on legal hold. Most corporate counsel have enacted some form of legal hold procedure, but very few have extended that process to include the rigor and control required to execute across people, processes and technology.

This whitepaper:

- Defines legal hold
- Highlights the most relevant sections of the amendments
- Provides basic advice for the creation of a litigation response plan
- Outlines how CommVault's Singular Information Management™ can be used to execute an effective legal hold across an organization's data topology

What is Legal Hold?

Legal hold is the process by which an organization protects and preserves all of the information that is potentially relevant to a particular legal matter. Legal hold encompasses people, processes and technology. People need to be notified that their information is on hold and that they should not delete any relevant information. Documented and repeatable processes need to be in place to protect evidence and ensure compliance. Technology needs to be engaged or disengaged to ensure that information is protected and not inadvertently destroyed.

A legal hold requires organizations to gather and preserve data from across the entire information landscape – record repositories, archives, databases, and most frequently, email.¹ The duty to preserve evidence supersedes all other retention/disposition guidelines, meaning that each system used to manage data within an organization must have some means of complying with a legal hold.²

¹ ESG Research Report: Digital Archiving; End-User Survey & Market Forecast 2006-2010, March 2006. According to an ESG survey of 206 companies, 77% reported that email and 50% reported that office files had been requested as part of a legal or regulatory action.

² In both *Napster, Inc. Copyright Litig.*, 2006 WL 3050864 (N.D. Cal. Oct. 25, 2006) and *United States v. Philip Morris USA Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004) the plaintiffs were sanctioned for failing to suspend their documented records retention policy.

Legal holds can be costly to execute, and improper or incomplete execution can lead to sanctions for spoliation (destruction) of evidence. A survey conducted by Fulbright and Jaworski states that “only 15% of U.S. Counsel [...] said their companies were well-prepared to handle a difficult e-discovery challenge as part of a contested civil matter or regulatory investigation.”³ Organizations need a solution that allows them to execute a repeatable and defensible legal hold strategy. The combination of a consistent, repeatable, and defensible process with the appropriate data management solution will dramatically decrease an organization’s exposure to sanctions.

Why is Legal Hold Important? A Case Study

One of the most frequently cited cases, *Zubulake vs. UBS Warburg, LLC*, provides a perfect example of how a company can get into trouble for failing to execute an effective legal hold. In February 2002, Laura Zubulake sued UBS Warburg for wrongful termination and gender discrimination.⁴ UBS denied Zubulake’s claims, but Ms. Zubulake got her case into court.

Case Summary: *Zubulake vs. UBS Warburg, LLC*

In July 2002, UBS produced 350 pages of documents from a period of seventeen months, including 100 pages of email from their active systems. Zubulake thought that more emails must have existed within UBS, most likely on backup tapes. This was based on her production of more than 450 pages of email from her own records. In January of 2003, UBS stated that a collection of 94 backup tapes contained the information for the relevant period. UBS claimed that the cost of discovery against all 94 tapes constituted undue burden and cost. The court agreed, and ordered UBS instead produce information from a sample of the 94. Five tapes, selected by Ms. Zubulake, were used as the sample set.⁵

Processing the five sampled tapes yielded an additional 6,203 emails, 1,075 contained the relevant search terms (“LZ”, “Laura”, “Zubulake”), and 600 were deemed responsive by UBS’s review. Based on the results of the sampling, Zubulake requested production from the remaining tapes. The total cost for the review and production of the five sampled tapes was \$19,003.43. The estimated total for production and review from the remaining tapes was projected to be \$273,649.39. Based on the anticipated cost of discovery from the remaining tapes UBS requested that the cost of review and production be shifted to Zubulake. The court used a weighted seven-factor⁶ test to determine if cost shifting was appropriate. The court ultimately ruled that the cost be shared, 25% paid by Zubulake, and 75% paid by UBS Warburg.⁷

³ Fulbright & Jaworski LLP: Third Annual Litigation Trends Survey polled 311 companies.

⁴ *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (“Zubulake I”) Ms. Zubulake had been a highly compensated equities trader prior to her termination (annual salary of \$500,000) , and subsequently was suing for \$13,000,000 in lost wages.

⁵ *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (“Zubulake I”)

⁶ *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (“Zubulake III”) Judge Scheindlin modified the seven-factor test set forth in *Rowe Entertainment, Inc. v. William Morris Agency, Inc* to include the following seven factors: “1. The extent to which the request is specifically tailored to discovery relevant information; 2. The availability of such information from other sources; 3. The total cost of product, compared to the amount in controversy; 4. The total cost of production, compared to the resources available to each party; 5. The relative ability of each party to control costs and its incentives to do so; 6. The importance of the issues at stake in the litigation; and 7. The relative benefits to the parties of obtaining the information.”

⁷ *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (“Zubulake III”)

During the restoration process, UBS realized that some of the tapes as well as certain isolated emails created after UBS had ordered the key players to stop deleting emails were missing. Based on the failure to comply with the preservation request, Zubulake sought sanctions for spoliation (penalties for the destruction of evidence).⁸ Based on the all of the evidence, or lack thereof, Judge Scheindlin ultimately sanctioned UBS. UBS was ordered to re-depose specific employees, restore additional backup tapes, pay some of Ms. Zubulake's attorney's fees, and the jury was instructed that they could assume that any of the emails not produced by UBS would have been favorable to Ms. Zubulake's case ("adverse inference sanction").⁹ Ultimately, Ms. Zubulake was awarded \$29 million.

In the end, *Zubulake vs. UBS Warburg, LLC* became less a case about gender discrimination and more about failed discovery operations. Something as simple as not keeping track of a few tapes, or making sure employees aren't deleting email, can cost significant time, energy and expense.

UBS had been on notice and had reported to the court that a specific number of relevant tapes existed, but when it came time to produce those tapes, seven had been lost. This constituted a direct violation of UBS' duty to preserve and thus led to the sanctions for spoliation. While this may seem like a worst case scenario, it could easily play out at many organizations.

Responding to Increased Legal Risk – What Data to Keep?

The Zubulake case sparks the question of what data to keep. The answers run the spectrum from "keep nothing" to "keep everything". "It goes without saying that a party can only be sanctioned for destroying evidence if it had a duty to preserve it."¹⁰ Those who opt to "keep nothing" must still collect all active, relevant information and put it on legal hold when litigation is reasonably anticipated. Those who have decided to "keep everything" have all of their data readily available, but face mounting storage costs and risk holding too much data. Additionally, those organizations that have adopted an over-broad strategy are faced with difficult decisions about what to delete and when. Many organizations feel that once they decide to keep data, they will never be able to reach a consensus about when it can safely be destroyed.

There are vigorous supporters of both approaches. Legal typically wants to keep less information. IT usually adopts a cautionary stance and keeps too much. Outside of specific regulatory requirements, most organizations adopt a strategy that falls somewhere in the middle. They attempt to maintain an archive housing key business records or email of frequently litigated employees – executives, accounting, finance, human resources, etc. Once these basic controls are in place, the organization is left to determine a means of executing a legal hold for the rest of their data. This is typically an ad hoc approach where the data is gathered as best they can when the legal hold is triggered. The ad hoc approach is

⁸ *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) ("Zubulake IV")

⁹ *Zubulake v. UBS Warburg LLC*, 382 F.Supp.2d 536 (S.D.N.Y. 2005) ("Zubulake V")

¹⁰ *Zubulake v. UBS Warburg, LLC* 220 F.R.D. 212 (S.D.N.Y. 2003) (Zubulake "II")

typically manual and inconsistent, creating concerns about chain of custody, completeness and data authenticity.

The Federal Rules of Civil Procedure

In an effort to provide organizations with guidance as what to keep and when to start keeping it, an industry group consisting of litigators, jurists, corporate counsel and vendors formed the Sedona Working Group (WG1) on Electronic Document Retention and Production.

WG1 created the “The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production”. The 14 Sedona Principles set forth by WG1 are cited in numerous court opinions and provide a baseline for the amended FRCP¹¹.

On December 1, 2006, after several years of review and comment, amendments were made to the FRCP to aid litigators, jurists, and organizations in effectively and efficiently fulfilling their e-discovery obligations. The “amendments address five related areas:

1. requiring parties to give early attention to issues relating to electronic discovery, including the form of production, preservation of information and problems reviewing electronic information for privilege;
2. relieving parties from searching for inaccessible electronic information, e.g., information on backup tapes;
3. retaining privilege protection for documents inadvertently disclosed;
4. requiring parties to agree on the form of production of electronic information or present the issue promptly to a judge for determination; and
5. limiting sanctions for loss of electronic information as a result of routine operation of computer systems, e.g., automatic purging of e-mails.”¹²

The following table summarizes the relevant amendments (underlined text denotes amended language):

Amendment	Topic	Summary ¹³
Rule 16(b) Rule 26(f)	Preparations for pre-trial conferences	“Requiring parties to give early attention to issues relating to electronic discovery, including the form of production, preservation of information and problems reviewing electronic information for privilege”
	Rule 16. Pretrial Conferences; Scheduling; Management (b) Scheduling and Planning. (5) provisions for disclosure or discovery of electronically stored information	
	Rule 26. General Provisions Governing Discovery; Duty of Disclosure (f) Conference of Parties; Planning for Discovery. “... confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for disclosures required by Rule 26(a)(1),	

¹¹ Federal Rules of Civil Procedure: These rules govern the conduct of all civil actions brought in Federal district courts. While they do not apply to suits in state courts, the rules of many states have been closely modeled on these provisions. Cornell Law School – Federal Rules of Civil Procedure <http://www.law.cornell.edu/rules/frcp/>

¹² The Third Branch, Newsletter of the Federal Courts, Electronically Stored Information Target of New Rules, Vol. 38, Number 11, November 2006

¹³ The Third Branch, Newsletter of the Federal Courts, Electronically Stored Information Target of New Rules, Vol. 38, Number 11, November 2006

	<u>to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan indicates the parties' views and proposals ..."</u>	
Rule 26(b)(2)(B)	Accessible vs. inaccessible information	Relieving parties from searching for inaccessible electronic information, e.g., information on backup tapes
	<p>Rule 26. General Provisions Governing Discovery; Duty of Disclosure (b) Discovery Scope and Limits. (2) Limitations (B) <u>A part need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information in not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party show good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for discovery.</u></p>	
Rule 34	Agreement on the form of production	Requiring parties to agree on the form of production of electronic information or present the issue promptly to a judge for determination;
	<p>Rule 34. Production of Documents, <u>Electronically Stored Information</u>, and Things and Entry Upon Land for Inspection and Other Purposes (a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, <u>test, or sample any designated documents or electronically stored information</u> – including writings, drawings, graphs, charts, photographs, <u>sound recordings, images, and other data or data complications stored in any medium</u> from which information can be obtained; translated, if necessary, by the respondent into a reasonably usable form... (b) Procedure. The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity . . . <u>The request may specify the form or forms in which electronically stored information is to be produced. Without leave . . .</u> (ii) <u>if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and</u> (iii) <u>a party need not produce the same electronically stored information in more than one form.</u></p>	
Rule 37(f)	Safe Harbor for IT operations	Limiting sanctions for loss of electronic data as a result of routine operation of computer systems, e.g., automatic purging of e-mails
	<p>Rule 37. Failure to Make Disclosures or Cooperate in Discovery; Sanctions (f) <u>Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.</u></p>	

FRCP Rule 37

Zubulake vs. UBS Warburg, LLC explores the risks associated with a failure to follow basic steps to meet a preservation request. It does not, however, cover how to handle extreme cases where automated processes cannot easily be stopped, or where such stoppage could dramatically affect the operations of the system, such as database maintenance, reuse of disk space by applications, or system cleanup associated with a simple user action.

In an effort to guide courts in the application of sanctions for the inadvertent destruction of data associated with the routine operation of computer systems, the Federal Judiciary has added part (f) to FRCP Rule 37, paraphrased from the table above as “the court may not impose sanctions for failing to provide data lost as a result of good faith IT operations”.

Rule 37(f) targets automatic processes that exist within the IT world:

- recycling of backup media,
- reuse of white space after the deletion of files,
- systematic updates to a file’s metadata by simple computer use,
- removal of data that is discarded because of age or lack of activity,
- and database maintenance operations that control storage consumption.¹⁴

Even with the protections offered by Rule 37 (f), organizations still need an effective legal hold mechanism.

When Does an Organization Have to Put Information on Hold?

An organization is not obligated to keep information just because it might be sued, however, when the organization reasonably anticipates litigation they need an efficient and effective means of putting all of the relevant information on hold. Determining when the hold starts is extremely subjective and best left to the organization’s legal team.¹⁵

¹⁴ Advisory Committee on Rules of Civil Procedure, May 2005, v. Sanctions for a Certain Type of Loss of Electronically Stored Information: Rule 37(f) <http://www.uscourts.gov/rules/reports.htm> The protections associated with the recycling of backup media are targeted at the reuse of media as a standard operating procedure, not the reuse of media that contains information relevant to a specific legal matter.

¹⁵ Turnbull, Tracey L. and Koesel, Margaret M., *Spoilation of Evidence, Sanctions and Remedies for Destruction of Evidence in Civil Litigation*. American Bar Association, 2006 “Generally, no duty to preserve evidence arises before litigation is filed, threatened, or reasonably foreseeable unless the duty is voluntarily assumed or imposed by statute, regulation, contract or another special circumstance. Absent notice of litigation, or another source of a duty to preserve evidence, a company or individual generally has the right to dispose of his own property, including documents and tangible objects, without liability.”

What Needs to Be Put on Legal Hold?

According to an ESG survey of 206 companies, 77% reported that email and 50% reported that office documents had been requested as part of a legal or regulatory action¹⁶, so it is safe to assume that most legal actions will require email and files. Beyond this basic assumption, determining what to put on hold is a difficult proposition.

Plaintiffs (accusers) will expect that every shred of information is put on hold, and the defense (accused) will want to keep the bare minimum. However, “[m]ust a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every back-up tape? The answer is clearly ‘no’. Such a rule would cripple large corporations, [...] that are almost always involved in litigation.”¹⁷ Despite an organization’s best efforts to manage and control the size and scope of preservation requests, they can still prove overwhelming. Below is an excerpt from the February 2005 preservation request submitted to Merck as part of the Vioxx litigation:

“interpreted broadly to include writings, records, files, correspondence, reports, memoranda, calendars, diaries, minutes, electronic messages, voice mail, E-mail, telephone message records or logs, computer and network activity logs, hard drives, backup data, removable computer storage media such as tapes, discs and cards, printouts, document image files, Web pages, databases, spreadsheets, software, books, ledgers, journals, orders, invoices, bills, vouchers, checks statements, worksheets, summaries, compilations, computations, charts, diagrams, graphic presentations, drawings, films, charts, digital or chemical process photographs, video, phonographic, tape or digital recordings or transcripts thereof, drafts, jottings and notes, studies or drafts of studies or other similar such material. Information that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and metadata, is also included in this definition. *Until the parties reach an agreement on a preservation plan or the Court orders otherwise, each party shall take reasonable steps to preserve all documents, data and tangible things containing information potentially relevant to the subject matter of this litigation.*”¹⁸

Organizations facing extremely broad preservation requests, like Merck, need relief in their efforts to respond to these types of preservation request. To assist litigators and corporations in fulfilling their duty to preserve, amendments were made to Rule 16(b) and 26(f) to force the topic of electronic discovery into pretrial conferences – meaning that parties in conference need to “discuss any issues relating to preserving discoverable information”. This is a motivating factor in the creation of a litigation response plan.

¹⁶ ESG Research Report: *Digital Archiving: End-User Survey & Market Forecast 2006 – 2010*, March, 2006.

¹⁷ *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (“Zubulake IV”)

¹⁸ Vioxx Products Litigation, Pretrial Order #1, Setting Initial Conference, Section 13. Preservation of Evidence. <http://vioxx.laed.uscourts.gov/>

Litigation Response Planning

Organizations working to meet the expectations set forth by the amended FRCP should develop a litigation response plan. A litigation response plan lays out the basic procedures necessary to execute on litigation events. A litigation response plan should be treated similarly to a disaster recovery/business continuity plan in that it is a process that is executed in crisis. The process should have executive visibility, be regularly reviewed for currency, and be practiced for effectiveness throughout the year. While the source of the crisis may be very different, i.e. lawsuit versus a server room fire, the teamwork, process, and coordination that is required to succeed is identical.

Litigation response plans are developed among business, legal and IT staff so that when a legal matter presents itself, the organization has a clearly defined process to determine what is put on hold. The business needs to identify the critical players; legal needs to assess the scope; and IT needs to execute the hold. Most organizations have a reasonable strategy to determine the first two steps, yet IT typically lacks the tools to execute. This process requires that IT have process and tools to effectively collect day forward data, gather and secure copies of the active data, and ensure that no potentially relevant backups are destroyed as part of the standard process. A cross-functional team in concert with a documented, rehearsed process creates a repeatable, defensible procedure for putting relevant information on legal hold.

A litigation response plan should include the following:

- A definition of the reaction team:
 - This team's members are resources with an understanding of the processes and procedures associated with their specific area of expertise: business, IT and legal. In most organizations the team will require numerous people, including alternates. Members of this team need to be senior, so that they can marshal resources and make decisions.
 - The primary objective of the reaction team will be to assist legal in determining key players, relevant data sources (email, files, laptops, trading systems, HR databases, etc.), and relevant time periods. This team will also need to knock down any hurdles that arise during the execution of the plan.
- A definition of the legal hold notification and enforcement process:
 - Once the key players are identified, they need to be notified, both in writing and verbally. In the fifth opinion coming from *Zubulake*, Judge Scheindlin increased the expectations on an organization's legal team such that, "when a duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored."¹⁹ Effectively, the counsel needs to not only notify the key players, but needs to regularly follow-up to ensure that the legal hold is being honored.
- The creation of an organization wide information map:
 - An organization wide information map will allow the reaction team to quickly target high value data – email, files, business applications, etc. The information map should also contain details about the organization's records retention processes, tape rotation policies, and archival policies, as well as details regarding any system that could automatically dispose of information, like file system,

¹⁹ *Zubulake v. UBS Warburg LLC*, 382 F.Supp.2d 536 (S.D.N.Y. 2005) ("Zubulake V")

- database or email pruning systems. The team should have copies of the policies as well as processes in place to ensure that they are both current and proactively followed.
- Key applications to include in the corporate information map.
 - Productivity
 - Email servers and local archives (PST/NSF files)
 - Records management systems
 - Collaboration (IM/discussion boards)
 - Web content management
 - Business
 - Business applications
 - Sales tracking
 - Accounting
 - Infrastructure
 - Archives (email/files)
 - Backup systems
 - Fax servers
 - Voicemail
 - Desktop Systems
 - Etc.
 - A definition of information that can and cannot be readily accessed and searched:
 - The amendment to Rule 26(b)(2)(B) implies a “two-tier” model for which information an organization is expected to readily search. The two tiers are categorized as information that is accessible and information that is “not reasonably accessible without undue burden or cost.” The expectation is that organizations will search and produce information that exists on active systems, but are not automatically required to search inaccessible sources. The two tiers are:
 - Accessible: Data that is accessed in the regular course of business. Email that exists in email servers or in employees personal archives, files that exist on file servers or on laptops/desktops, archival systems that are indexed, content management repositories...
 - Inaccessible: Data that is “not reasonably accessible without undue burden or cost”. “Backup tapes intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching, legacy data that remains from obsolete systems and is unintelligible on the successor systems; data that was ‘deleted’ that remains in fragmented form, requiring a modern version of forensics to restore and retrieve; and databases that were designed to create certain information in certain ways and that cannot readily create very different kinds or forms of information.”²⁰
 - Organizations need to approach the designation of “inaccessible” data very carefully. If an organization declares a collection of data as inaccessible and does not search it as part of the discovery request, they must inform the requestor that this pool was not searched. If the requestor feels that the importance of the data out-weighs the burden, they can request that the court compel the search and production of data from that repository.
 - As part of the litigation response plan and the organization’s information map, the organization needs to understand how their data fits into this model. Additionally, this designation needs to be applied consistently. Designating a source that contains favorable information accessible in one case, but inaccessible when information is unfavorable will not be well received by the court.
 - A documented, repeatable, and defensible means of gathering all of the key player’s relevant data and placing it in a protected state – a state of legal hold.

²⁰ Advisory Committee on Rules of Civil Procedure, May 2005, ii. Discovery of Electronically Stored Information that is Not Reasonably Accessible: Rule 26(b)(2)(B) <http://www.uscourts.gov/rules/reports.htm>

CommVault's Solution Suite

The CommVault software suite provides organizations with a simple, holistic system for managing corporate information. The amendments to the FRCP are different than records retention regulations such as SEC 17a-4, HIPAA, DOD 5015.2, FOIA, and SOX, in that they do not direct a specific retention requirement or actually even mention retention. The amendments to the FRCP instead confirm that organizations need to understand how they store all data across the enterprise (e.g active data, data on ten year old tapes, etc.); clarify retention policies; and identify automated processes that might delete information.

CommVault's solution is uniquely positioned as a single, unified data management software platform. By leveraging the CommVault Common Technology Engine (CTE), organizations can reduce the number of repositories that they have to manage and search in response to litigation. CommVault's single platform for data protection, data replication, and data archiving allows organizations to focus on managing, producing and protecting information because that information is managed in a single repository.

CommVault's Singular Information Management™ Platform offers:

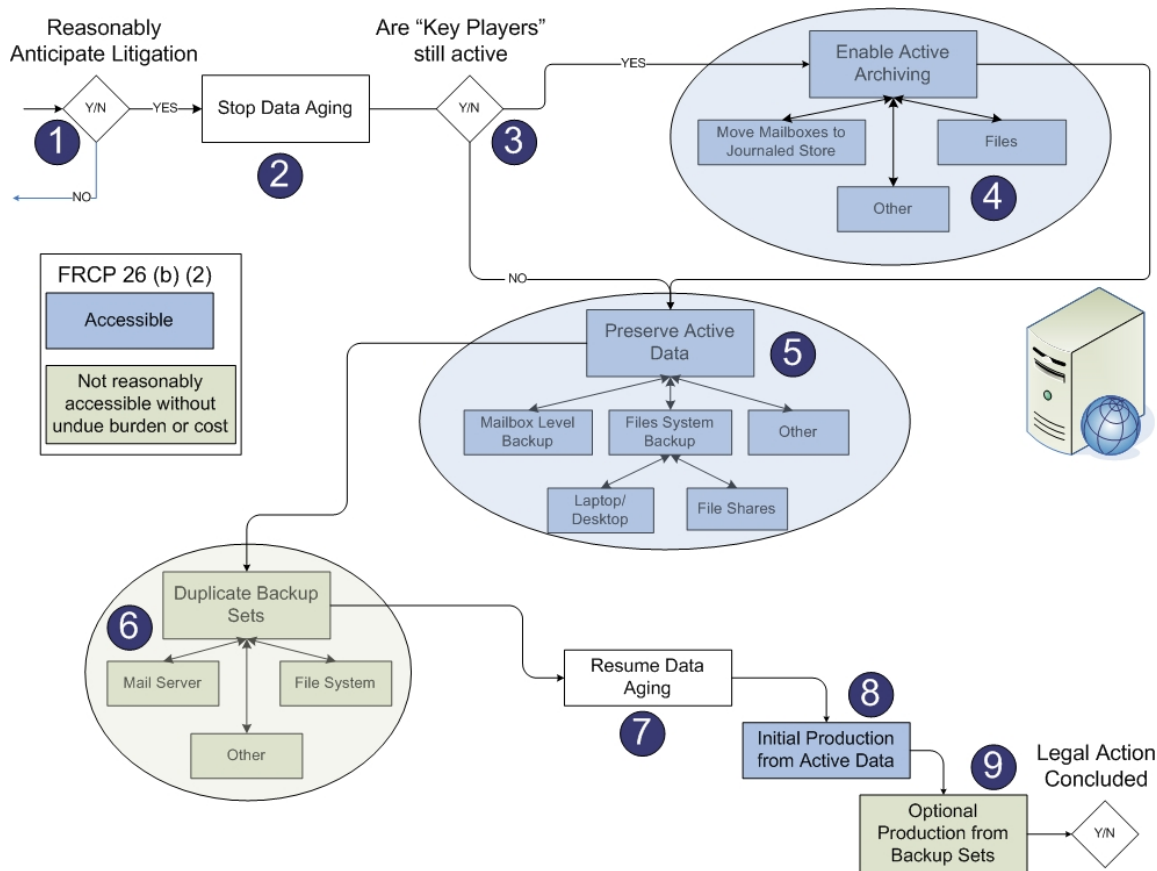
- **Legal Hold Support:** CommVault Galaxy™ Backup & Recovery enables customers to respond to anticipated legal action by collecting and content-indexing relevant data in a user's mailbox or files and placing it on legal hold – via standard backup policies
- **Data Archiving:** CommVault's data archiving solution includes Data Archiver™ for real-time collection of data from the Exchange, Lotus Domino, SharePoint and file system data, and Data Archiver Compliance Option for the scheduled collection of both e-mail and files based on a variety of metadata parameters. These capabilities, combined with content indexing, give organizations more options to organize and retain business records.
- **Media Management:** CommVault's native media management provides a robust mechanism to logically manage data. CommVault VaultTracker™ monitors the location of removable media, manages library slots for easy media access, prompts for media rotation to ensure compliance with policies, manages foreign tapes, and automates the rotation of media back on-site for reuse and retirement.
- **Audit-ready Reporting:** CommVault also provides audit-ready reporting of data management operations, as well as data and tape locations, to enable legal and IT teams to answer questions during pre-trial conferences.

CommVault's Legal Hold support provides a unique approach to meeting the expectations of the FRCP and the needs of the organization. CommVault provides both the tools and techniques to:

- actively archive end user data;
- reactively gather all of the active and accessible information into a readily searchable format;
- manage media to ensure protection from sanctions if discovery extends to backup tapes.

Legal Hold Process with CommVault Suite

An effective legal hold process requires the coordination of IT and legal. Most organizations have a solid process on the legal side, but lack a consistent and repeatable process on IT side. CommVault's technologies can be applied to execute a repeatable and defensible legal hold.



1. Does the organization anticipate litigation? The trigger for a legal hold is a subjective process, and best left to the legal team to determine when it should begin. The litigation response plan should be the roadmap for execution once the hold is ordered. This initial activity from the legal team should define the scope: who, what, when, and where. The CommVault legal hold process will provide the technology to execute the hold – the ‘how’.

When the process starts, the key players, the relevant location of data, and the date ranges in question need to clearly understood. At this stage it is more important to gather and protect the information than try to be very specific in what is gathered.

2. Pause the automatic tape rotation and data aging processes, setting the extended retention attribute on the appropriate jobs. This attribute will prevent pruning of the selected jobs until the attribute is manually removed. This attribute is selectively applied to appropriate jobs, focusing

the hold only on the relevant information. This will ensure that the potentially relevant data is not inadvertently destroyed. While the addition of FRCP Rule 37(f) provides some protection, this is still a necessary step. The swift execution of the steps 3-6 will decrease the amount of time that these processes need to be paused.

3. Are the “key players” still active and/or does the litigation include day forward data? At this point, the organization needs to determine if the scope of the request requires they attempt to capture everything from a day forward perspective. Based on the nature of the case this may be completely unnecessary, however, as we saw in the *Zubulake* opinions, employees who do not follow the legal hold instructions and delete relevant emails, open the whole organization up for sanctions.²¹
4. Optionally enable real-time collection of employee’s communications by moving their mailbox into a segment of the messaging environment that uses journaling. Once the “key players” mailboxes have been moved into journaled mail store, CommVault’s Data Archiver module can be used to archive, index and preserve the journaled messages under an appropriate retention policy. Real-time collection of all sent and received emails provides organizations with a complete audit trail of targeted emails. The addition of content indexing of all message metadata and attachment content provides a simple and robust solution for capturing, archiving, and content searching real-time electronic communications. (This technology can be combined with 3rd party solutions that provide IM-capture functionality).
5. Gather the active information by creating case-specific preservations sets. Active data is typically considered the information that is used and accessible in the regular course of business – email in mailboxes, PST files, .nsf files, files on files servers, desktops/laptops, data contained in archives, both online and near-line, SharePoint, etc. This can be a one-time capture or scheduled to continue for a prescribed period depending on the requirements associated with the lawsuit.

Sub-steps might include:

- a. Perform a targeted mailbox level backup with content indexing using the standard CommVault Galaxy mailbox level backup agent.
- b. Perform targeted file system backups with content indexing for any share, desktop or laptop with the standard file system agent.²²
- c. Perform backups of any other resources that may be potentially relevant to the case, such as databases, SharePoint, server logs, web sites, etc. using a variety of standard CommVault database and application server agents.
- d. Search any archives for information associated with key players and copy that information into the legal hold storage policy. Data Archiver is readily searchable through a robust content indexing search interface. The results of these searches can easily be exported into Exchange and subsequently included as part the preservation set.

²¹ *Zubulake v. UBS Warburg LLC*, 382 F.Supp.2d 536 (S.D.N.Y. 2005) (“Zubulake V”)

²² Applies to Windows file systems only.

Copying all of the relevant information into a dedicated legal hold storage policy minimizes the disruption associated with stopping tape rotation and data aging. Additionally, by scheduling search and export operations from the archive, the relevant information can be extracted from the general-purpose archive and moved into the case specific preservation sets. This ensures that data collected by Data Archiver can be disposed in accordance with the existing disposition schedule.

Amendments to Rule 26 (b)(2)(B) were intended to reduce the burden of searching, reviewing, and producing information from difficult to access data. The expectation is that the majority of litigation should be addressable by information that is active and accessible. Active and accessible data may be easier to get to, but it still provides its challenges. CommVault's solution suite reduces the risk of end users intentionally or unintentionally destroying their active data, by copying the information in its native format into dedicated storage policy within the CommVault system. With any of the standard CommVault agents, but most frequently the messaging or file system agents, object level backups can easily be performed. This process provides several benefits:

1. Copies the active information as it existed when the legal hold was triggered
2. Stores the items in their original format
3. Content indexes the documents, providing a powerful, yet simple search of the gathered data.

Amendments to FRCP Rule 34 (b) requires that "a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable". Otherwise, the original or native format is now the default form for producing electronically stored information. CommVault's long history of data protection provides a proven track record for collection and recovery of the items in their original format. This history also ensures that all activity is fully audited, including: item level tracking, comprehensive job history reporting for both collection and retrieval operations, and media and copy management information such that the location of each item can be determined throughout its lifecycle.

6. Protect the relevant backup jobs. The "two tier" system of accessible and inaccessible information associated with FRCP Rule 26(b)(2)(B) attempts to reduce the burden on organizations by controlling expectations associated with the search and discovery against difficult to access repositories. However, it does not eliminate their need to preserve potentially relevant information contained in those repositories, like backup media, as a court can still compel an organization to produce regardless of cost or difficulty. Organizations must have a way to protect and optionally duplicate the potentially relevant backup data.

CommVault's media management layer allows operators to create copies of the relevant backup jobs by creating a case-specific copy set. Creating case-specific copy sets allows organizations to hold only relevant information, eliminating the need to hold a single tape that could have multiple datasets of discoverable information. This model allows organizations to avoid the situation where tapes being held for one case might be discoverable in another case. Additionally, for each job that is copied into a preservation set, the extended retention flag can be set. The extended retention flag ensures that the data will not be inadvertently aged if a policy is mistakenly changed. This also provides an annotation in the media reports that provides a specific reference to exactly what is held in a protected state.

7. Resume the automatic tape rotation, remove the extended retention flag from the original backup copy, and commence the data aging processes. Gathering copies of the active information and duplicating relevant backup jobs minimizes the disruption to the regularly scheduled operations. It also allows organizations to maintain the minimum amount of potentially discoverable information.
8. Perform the initial discovery from the collected information. CommVault's solutions – mailbox and file system backup, Data Archiver – all offer content indexing of file content, email attachments, and email metadata. CommVault's integrated full text search simplifies the culling process by allowing the result set to be further refined through a powerful search engine. The integration of the collection, protection and search of the active data ensures that organizations can most cost effectively meet the expectations defined in Rule 26(b)(2)(B). By first targeting active information, organizations, as well as the courts, hope to be able to fulfill the majority of the discovery requests, reducing the cost and burden of discovery against difficult or costly to access information.
9. Declaring system backups as inaccessible is possible under amended Rule 26 (b)(2)(B), but it does not eliminate the chance that an organization might be compelled to produce from those sources. By gathering and protecting the potentially relevant backups in step 6, the organization has protected itself against sanctions for spoliation. By preserving and protecting the "inaccessible information" as part of a targeted copy set, the organization is prepared in case they are compelled to produce information from those sources. Once compelled, the organization has the data in a format whereby they can start the restoration and data extraction process.

Conclusion

The amendments to the FRCP offer no retention requirements and do not mandate a specific technology solution. These amendments simply advocate good data management policy and an organizational awareness as to the best practice for communicating and responding to electronic discovery requests.

Organizations should:

- Prepare now for pre-trial conferences by understanding where and how the organization stores all of its information (Rule 16(b) and 26(f))
- Define how the organization categorizes accessible vs. inaccessible data (Rule 26(b)(2)(B))
- Prepare a litigation response plan, and practice in concert with disaster recovery and business continuity plans
- Recognize that an effective legal hold requires collaboration between legal, IT and business

The combination of awareness with a consistent and repeatable process will provide an organization with the tools and techniques necessary to execute when litigation occurs.

CommVault's solutions provide a unified data management platform from which an organization can fulfill the expectations of the FRCP. CommVault manages data using logical storage policies to facilitate intuitive data management and eliminate the requirement to manage each host's retention policy independently. This logical grouping facilitates fewer, and more accurate retention policies. Both of these strategies provide for continuous best practice data management.

CommVault then provides all of the tools and techniques necessary to execute an effective legal hold:

- Archive real-time communications for ongoing cases
- Collect active information across email, file servers, desktops, laptops and application servers, copy that information into a dedicated storage policy where email, attachments and files can all be content indexed
- Copy relevant backup sets to minimize the risk of sanctions
- Produce active data from a pool of content-indexed information
- Provide reports that demonstrate compliance with legal and regulatory requirements

CommVault's Singular Information Management™ platform encompasses backup, archive, and media management, and therefore enables the streamlined creation of comprehensive litigation response plans, and the efficient execution thereof, to effectively reduce the costs and risks associated with litigation.