By Elaine M. Adam and Lori A. Lofano

Creating an Effective Litigation Hold Plan

Although the litigation hold and preservation process might be viewed as straightforward and ministerial, it is far from that.

On the contrary, when the Federal Rules Amendments take effect as of December 1, 2015, under the new Rule 37(e), the focus of spoliation motions will be on the "reasonable steps" each party took to preserve relevant information. As we discuss in this article, there are many critical moving parts to the litigation hold process that should be incorporated into a company's routine business practices. Doing so is mandatory if a corporation wants to ensure it has effective preservation processes in place that will stand up to sanctions motions when challenged in court. Most importantly, these processes should be formalized into a written, routine, and repeatable litigation hold plan that should include:

(1) a written litigation hold form;
(2) a written process for the identification of employees who will be considered "key custodians" and whose data will be preserved;
(3) written policies to suspend the automatic destruction of data; and
(4) written guidelines describing the roles and interactions of the legal hold team assigned to each case.

Even though a corporation may routinely issue written litigation holds, have written processes for the effective identification of key custodians whose data will be preserved, and have written policies to suspend the automatic destruction of data, the corporation still may have an incomplete litigation hold plan if it does not have an effective legal hold team in place. An effective team is not limited to individuals within the corporation, but rather should include members of the corporation's information governance or cyber security team, IT department employees or outside IT vendors, records management department employees, human resource department employees, in-house counsel, and outside counsel.

Courts increasingly expect that outside counsel will be actively involved in all aspects of the litigation hold plan. The corporation and the attorney may face sanctions if outside counsel does not "actively supervise and manage" its client's litigation hold activities. *Pacific Packaging Products, Inc. v. Barenboim*, No. 09-4320, 2014 Mass. Super. LEXIS 46 (Mass. Super. Ct. Apr. 1, 2014). Outside counsel must be actively involved in all aspects of the litigation hold plan, beginning when the litigation is first reasonably anticipated. *Alter v. Rocky Point Sch.* Dist., No. 13-1100 (JS)(AKT), 2014 U.S. Dist. Lexis 141020 (E.D.N.Y. Sept. 30, 2014) Initially, outside counsel should be involved in implementing the hold and interviewing custodians. Once the hold is in place, outside counsel should re-confirm on a regular basis that relevant data is being preserved and that the hold continues to remain in effect. It does not matter how technologically sophisticated the corporation is and how intimately in-house counsel and the IT department are involved in the litigation hold process; outside counsel also needs to be involved in all aspects of this process.

The goal of this article is to provide information regarding the key steps in implementing a litigation hold plan, including when to issue a hold and when to lift it, identification of key custodians to include within the scope of the hold, and how in-house and outside counsel can work with the corporation's IT department more effectively. We will also discuss how the forthcoming amendments to the Federal Rules of Civil Procedure may impact the implementation of litigation holds in federal cases.

Triggering the Duty to Preserve

The duty to preserve is triggered upon actual or anticipated notice of litigation. *See, e.g., Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.* 244 F.R.D. 614, 620 (D. Colo. 2007) (*citing Zubulake v. UBS-Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). For a corporate defendant, "actual or anticipated notice of litigation" will often mean the date the corporation's agent accepts service of process. *See, e.g., Quantlab Techs. Ltd. v. Godlevsky*, No. 4:09-CV-4039, 2014 WL 651944 (S.D. Tex. Feb. 19, 2014).

However, service of process is not the only method by which a corporation can be deemed to have notice of anticipated litigation. Rather, the duty to preserve may be triggered when a corporation receives any written or oral notification that would indicate that litigation is likely. *See, e.g., AJ Holdings Grp., LLC v. IP Holdings, LLC*, No. 600530/2009, 2014 WL 4652899 (N.Y. Sup. Sept. 15, 2014)(holding plaintiff's duty to preserve began the date its counsel sent

■ Elaine M. Adam is senior counsel in Bowman and Brooke LLP's Los Angeles, California, office. She is former general counsel for Makita U.S.A., Inc. Her practice is focused on defending automobile manufacturers in product liability claims. She has handled all aspects of case management, law and motion, and has been involved in extensive discovery issues and document productions for manufacturers of automobiles, power tools, and off-road recreational vehicles. Lori A. Lofano is a partner in the Phoenix, Arizona, office of Bowman and Brooke LLP. Her practice is focused on implementing and executing uniform discovery and e-discovery processes for her clients. Ms. Lofano has extensive experience in resolving discovery and e-discovery issues in catastrophic injury and other high exposure products liability cases throughout the United States.

defendants a letter regarding the early termination of the licensing agreement at issue in the case and sanctioning plaintiff with adverse inferences both at summary judgment and at trial for plaintiff's gross negligence in deleting relevant data as a result of its failure to implement a litigation hold). *See also, Apple Inc. v. Samsung Electronics Co., Ltd.,* 881 F. Supp. 2d 1132, 1150 (N.D. Cal. 2012) (duty to implement a litigation hold began when a meeting was held between the corporations at which information was presented about the alleged infringement of certain patents, not after suit was filed eight months later). In each of these cases, the court held that the notice was sufficient to advise the parties that litigation could reasonably be anticipated. Because notice of potential litigation triggers the duty to preserve, as soon as a corporation becomes aware that a lawsuit is *reasonably likely* to be filed against it, the duty to preserve is triggered and the corporation must immediately begin to put a litigation hold plan in place.

Identifying Key Custodians

Identifying key custodians is critical in the litigation hold process. If the organization does not issue the hold to key custodians, and their data is not preserved, the organization can run into serious problems later with sanctions. This section will discuss who key custodians are, why they are considered key custodians, and how their data must be preserved.

The concept of the key custodian is not a new or novel one; rather, it is rooted in the Federal Rules of Civil Procedure. As early as 2003, in *Zubulake v. UBS Warburg LLC*, the court refers to key custodians as "key players." *Zubulake,* 220 F.R.D. 212, 216 (S.D.N.Y. 2003). These are the employees who are "likely to have discoverable information" that the disclosing party may use to support its claims or defenses. *Id.* at 217–18 (citing to Fed. R. Civ. P. 26(a)(1)(A)).

Moreover, identifying key custodians is an iterative process. This is illustrated no more clearly than in *Apple, Inc. v. Samsung Electronics Co., Ltd.,* 881 F. Supp. 2d 1132 (N.D. Cal. 2012). There, the initial hold was issued to 27 employees, but grew to over 2,700 employees as the company's fact finding during the legal hold process revealed information identifying many additional custodians. Furthermore, the scope of the hold language was expanded to include language that, if in doubt whether to preserve a document, "you are instructed to retain them." *Id.* at 1143. The *Apple* case stands for the proposition, therefore, that even after a hold is issued, the organization must stay vigilant to identify additional custodians and amend the hold language if necessary.

The *Apple* case stands for the proposition, therefore, that even after a hold is issued, the organization must stay vigilant to identify additional custodians and amend the hold language if necessary.

Indeed, failure to identify key custodians and preserve their data can result in sanctions. *Day v. LSI Corp.,* No. CIV 11-186-TUC-CKJ, 2012 WL 6674434 (D. Ariz. Dec. 20, 2012), offers a good example of what not to do. *Day* was a breach of employment contract case in which the computer files of LSI employee Stanley Skelton were destroyed when he left the company. Skelton, who was involved in the hiring and performance reviews of the plaintiff, Kenneth Day, was not issued a legal hold. But the court determined that Skelton was a key custodian because of his involvement in Day's hiring and Day's decision to leave LSI—claims that were central to Day's lawsuit. The court found that Skelton's involvement "should reasonably have been known" to LSI and thus his data should have been preserved. *Id.* at ¶11. As this case illustrates, corporations should always take a practical look at the duties and responsibilities of each key custodian when issuing the hold, and definitely before destroying any data of a potential key custodian. *See also, In re Pradaxa (Dabigatran Etexilate) Prod. Liab. Litig.*, No. 3:12-MD-02385-DRHSCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013) (Defendants ordered to pay plaintiff's fees and costs associated with litigating defendants' discovery violations where defendants failed to issue a litigation hold for certain key custodians for one and a half years and failed to include a key custodian within the scope of a separate hold).

Additionally, the company must take proper steps to regularly monitor the litigation hold and ensure the key custodians' compliance with the hold. *See In re Ethicon, Inc.*, 299 F.R.D. 502 (S.D.W.Va. Feb. 4, 2104). It is not enough for the company to identify custodians and issue the hold; the company must follow up with custodians regularly to ensure they are adhering to the terms of the hold. Further, the company needs to go the extra step to educate employees regarding preservation of data—not only what data must be preserved, but how to preserve it and how not to inadvertently destroy it.

Importantly, the duty to preserve does *not* extend to employees who are "unlikely candidates" to have relevant documents. *See AMC Tech., LLC v. Cisco Sys., Inc.,* No. 11-CV-3403 PSG, 2013 WL 3733390 (N.D. Cal. July 15, 2013). The company must look at the issues in the case and then look at the job function and responsibilities of the employee. For example, if the issues in a case concern the formation of a contract, an employee who was not involved in contract negotiations, may be an unlikely candidate to have documents relevant to the hold. As such, that employee would *not* be a key custodian because the scope of duty to preserve is "confined to what is reasonably foreseeable to be relevant to the action" and "is not limitless." *See id.* at ¶3.

Third-Party Key Custodians

An organization's duty to issue a hold sometimes extends beyond its own employees to third parties it has "control over and access to." *See Haskins, v. First Am. Title Ins. Co.*, No. CIV. 10-5044 RMB/JS, 2012 WL 5183908 (D.N.J. Oct. 18, 2012). *Haskins* involved an alleged scheme by a title company to overcharge customers for title insurance. The third party, which the court determined was subject to the hold, was the title abstract company that had contractual relationship with First Amer-

ican Title. In determining whether the abstract company was a key custodian, the court looked to the agency relationship that was created by the contract between First American Title and the title abstract company. This relationship gave First American control over and access to the title abstract company's data. The important takeaway here is to take a careful look at third parties and the relationship those third parties have with the organization. Do the facts and circumstances surrounding the relationship between the third party and the organization give the organization "control and access to" the third party's data? If so, they are key custodians, and even if they are not employees, the hold will extend to them.

When Key Custodians Leave

After a corporation has identified key custodians, it is equally important to make sure to preserve the data of those custodians—even after they leave the company. This is no more obvious than when it comes to mass layoffs. This is a time when the deletion of relevant data in departing employees' files can occur in the blink of an eye. The 2014 *Actos* decision exemplifies these issues. *See In re Actos (Pioglitazone) Prod. Liab. Litig.,* No. 6:11-MD-2299, 2014 WL 2872299 (W.D. La. June 23, 2014). *Actos* is a 2,600-member product case arising out of the risk of cancer from ingesting the drug Actos. On the issue of spoliation, the court found that 46 employees were key custodians, and their files should not have been deleted after the litigation hold was issued. The court found them to be key custodians because they were high-ranking employees who were involved in the day-to-day marketing of distribution of the product. In that capacity, they should have been aware of the cancer risk of the drug at issue in this case. The court found spoliation and allowed the evidence of spoliation to go to the jury. *Actos* provides a crucial takeaway: always be mindful during mass layoffs to preserve data of key custodians. Look at the facts and circumstances surrounding each employee who is terminated and determine if they are key custodians whose data, including all emails, must be preserved.

Not only must companies be mindful not to delete data of departing key employees, but they must be mindful of where the data is located and how not to inadvertently delete it. For example, deletion of key custodians' data can easily occur during a computer system migration. This was the case in *E.E.O.C. v. Ventura Corp.*, No. CIV. 11-1700 PG, 2013 WL 550550 (D.P.R. Feb. 12, 2013). In this unlawful employment practices case, the key custodians were managers, who were involved in plaintiff's hiring and employment at Ventura Corporation. The court determined that these managers were "key decision-makers," and as a result, their files should have been preserved even after they were terminated. However, after the managers left the company, their files, including emails, employment applications and resumes, were lost during a computer system migration. The court said that Ventura should have "reasonably anticipated" the litigation based on these managers' emails. Because the migration took place after Ventura's duty to preserve arose, Ventura should have been especially mindful to preserve its managers' data.

> It is not enough for the company to identify custodians and issue the hold; the company must follow up with custodians regularly to ensure they are adhering to the terms of the hold.

Key Custodians Used to Craft Search Terms

Key custodians may also be helpful in crafting the search terms used to locate potentially relevant data and to suspend the automatic destruction of data. *See Procaps S.A. v. Patheon Inc.,* No. 12-24356-CIV, 2014 WL 800468 (S.D. Fla. Feb. 28, 2014); No. 12-24356-CIV, 2014 WL 1047748 (S.D. Fla. Mar. 18, 2014). *Procaps* involved a motion for a forensic analysis of Procaps' electronic media. In granting this motion, the court said the "basic rule" is counsel must carefully craft search terms with input from the corporation's key custodians. *Procaps* at ¶4. The court determined that the failure of Procaps' counsel to meet with IT personnel to discuss the potential locations of discoverable electronically stored information ("ESI") contributed to Procaps' inadequate preservation. Moreover, the court issued a very detailed and extensive order in which it specifically named custodians whose files had to be searched, as well as ordering Procaps to retain an e-discovery vendor to conduct an extensive forensic analysis of Procaps' data sources. In addition, the court ordered Procaps counsel to personally interview the custodians and to disclose potential data sources to opposing counsel. Procaps' counsel also had to work with opposing counsel to come up with a list of search terms that vendor would run against document collections.

Working Effectively with Information Technology Departments

The company's IT department is an integral part of the legal hold team from the beginning. IT must be consulted early in the litigation hold process: to identify relevant data sources and stop the company's automatic deletion processes in order to preserve relevant data. The IT department knows how information flows to and from the company—how it communicates with related entities, customers, and the public. IT also knows what structured data sources exist, and can connect counsel with business users who can help identify any relevant information that exists in those sources.

Vincente v. City of Prescott, 2014 U.S. Dist. LEXIS 109790 (D. Ariz., Aug. 8. 2014), illustrates just how important IT is in the legal hold process and how the courts see IT's role in this process. In *Vincente*, the city did not notify IT of the hold, although it had notified key custodians. Furthermore, the city did not ask IT to help the custodians collect data. As a result, the court found that the data preservation was inadequate and "plainly deficient" and awarded attorneys' fees. *Id.* at ¶9.

Likewise, in *Kirgan v. FCA LLC*, No. 10-1392, 2013 WL 1500708 (C.D. Ill., Apr.

10, 2013), the court found that IT was essential in preserving data. In *Kirgan*, two managers, who were involved in the decision to terminate Kirgan, routinely deleted their daily electronic calendar entries even after the litigation hold was issued. These entries included details of who attended meetings, the content of those meetings, and even attached relevant documents. The court found that these managers were key decision makers in the termination, and thus their data should have been preserved. The court issued a spoliation instruction allowing the jury to draw a negative inference from the failure to preserve. Had IT been consulted, however, and suspended the automatic deletion process of these calendar entries, there likely would not have been a spoliation issue. *See also, Knickerbocker v. Corinthian Colleges*, 298 F.R.D. 670 (W.D. Wash. 2014) (defendant and defense counsel ordered to pay monetary sanctions to plaintiff, in addition to paying attorney fees and costs, where defendant failed to follow its standard practice and issue a litigation hold at the commencement of anticipated litigation, failed to ask key employees to preserve relevant documents, and deleted potentially relevant email after the commencement of litigation).

Identifying Data Sources: Personal Accounts and Less Likely Data Sources

As discussed earlier, a corporation must include within the scope of its litigation hold any data sources that are within the organization's control and likely to contain relevant data. Because most employees will have their own personal accounts, including email and social media accounts, the company must determine whether such accounts fall within the organization's control and, if so, whether they are likely to contain data within the scope of the hold. Specifically, personal email and social media accounts may be subject of the hold if the company knows or should know that these personal accounts are being used for company business. In *Puerto Rico Tel. Co. v. San Juan Cable*, LLC, No. CIV. 11-2135 GAG/BJM, 2013 WL 5533711 (D.P.R. Oct. 7, 2013), the plaintiff provided sufficient evidence to demonstrate that San Juan knew that its former officers used their personal email accounts for many years to conduct company business. As a result, San Juan had a duty to preserve those personal emails that contained data relevant to the hold.

Moreover, the company must clearly communicate in the litigation hold that the hold applies not only to business applications but to personal accounts as well, where those accounts relate to the subject of the hold. Personal accounts would include not only email, but also applications such as text messages and social media. In *Zest IP Holdings, LLC v. Implant Direct Mfg.*, LLC, No. CIV. 10-0541-GPC WVG, 2013 WL 6159177 (S.D. Cal. Nov. 25, 2013), a key senior employee admitted she had a personal AOL account that she used for both work and personal purposes. The employee admitted deleting email on the account that was work-related, because she was never advised to retain such email. The court issued an adverse inference instruction and monetary damages for the company's failure to preserve email from this account.

While personal email accounts seem like an obvious data source, there are also data sources that are less obvious to the lay person. The corporation's IT department will know both the obvious, as well as the less obvious, data sources that must be reviewed for relevant information to preserve. Obvious data sources would include hard drives, back-up tapes, flash drives, and company email. Less obvious, and less likely, data sources would include instant messengers and social media—including Twitter accounts, LinkedIn, and Facebook—and also Cloud-based applications, such as Salesforce, which is a customer relationship management product used by some companies.

Indeed, in *Robinson v. Jones Lang LaSalle Americas Inc.*, No. 3:12-cv-00127-PK, 2012 U.S. Dist. LEXIS 123883 (D. Or. Aug. 29, 2012), the court saw no reason for different standards for the discoverability of communications through text or other social platforms versus more traditional communications such as email. As *Robinson v. Jones Lang* demonstrates, the litigation hold team must determine whether the instant messages are likely to contain data relevant to the hold. The organization must involve IT in identifying not only traditional company data repositories like company email, but also less likely data sources, like instant messages on a company system that are likely to contain relevant data to the hold. Moreover, less likely data sources cannot be overlooked in document collections. For example, a company's own website, and any data that is on or downloaded from site can be considered a data source and thus subject to the hold. *See Nacco Materials Handling Grp., Inc. v. Lilly Co.,* 278 F.R.D. 395 (W.D. Tenn. 2011). This would also include server logs and internet history. *See Helget v. City of Hays,* No. 13-2228-KHV-KGG, 2014 WL 1308893 (D. Kan. Mar. 31. 2014).

When IT Is an Outside Vendor

Many times, the information technology function is not a department within the company, but rather one delegated to an outside vendor. Although companies may have a variety of reasons for outsourcing their IT functions, the bottom line is that even when IT is an outside vendor, it must be notified of the legal hold. And just as with an IT department within a company, counsel must notify an outside IT vendor of the litigation hold early in the process and work with the vendor often during the litigation hold process to identify data sources, suspend automatic deletion functions, help craft search terms, and search for relevant data.

In *Sekisui American Corp. v. Hart*, 945 F. Supp. 2d 494 (S.D.N.Y. 2013), the company used an outside vendor for all IT functions, including preservation of data and suspension of email deletion. Sekisui American Corp. delayed instituting the litigation hold for more than 15 months after receiving notice of the claim. During that time, the IT vendor deleted the president's and another key employee's emails. The company argued that the IT vendor, which was not notified of the hold for six months, deleted these emails to free up space on a server. The court, however, found that the deletion rose to the level of "gross negligence" even if it was not willful, and issued an adverse inference instruction. The important takeaway here is that when an organization has delegated its IT function to an outside vendor, notification

to the vendor *must* be part of the organization's written protocols for preserving data should a legal hold be issued.

Lifting the Litigation Hold

Lifting the litigation hold at the appropriate time after the conclusion of litigation is as important as implementing a hold. Courts will rely in part on the fact that a corporation has not lifted a hold in determining when the corporation's duty to preserve first arose in subsequent litigation that involves the same issues. *See In re Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig.*, 299 F.R.D. 502 (S.D.W. Va. 2014). And if the corporation does not timely lift a hold, a court overseeing subsequent litigation involving the same product may look to the earlier hold as having continuing effect. This gives the opposing party an opportunity to claim information lost in the interim was spoliated.

Determining the appropriate time to lift the hold will depend upon how the case ends. After a case has reached a definitive termination, including any appeals, the corporation should lift the litigation hold. If the case settles, the settlement agreement may include a provision that expressly provides for the termination of the litigation hold. If litigation was threatened, but never commenced, the hold may be lifted when the corporation makes a firm decision not to file suit; or, if the corporation was a potential defendant, when the corporation becomes aware of a firm decision not to file suit and the statute of limitations has run. *See* The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 Sedona Conf. J. 265, 287 (2010).

In all of these scenarios, there may be extenuating circumstances that require the litigation hold to remain in place. If a case ends, the corporation must first ensure that there is no other current or anticipated litigation that would require the hold to remain in place before making any provision to lift the hold.

The Effect of Federal Rule Amendments on Litigation Holds

The amendments to the Federal Rules of Civil Procedure are scheduled to take effect on December 1, 2015. Under the amended Federal Rules, the scope of discovery must be proportional to the needs of that case. *See* proposed amendment to Fed. R. Civ. Proc. 26(b)(1), available at http://www.uscourts.gov/file/document/congress-materials. Because the litigation hold is the tool by which documents relevant to discovery are managed, this rule may also be used to reflect the scope of litigation holds.

> The important takeaway here is to take a careful look at third parties and the relationship those third parties have with the organization.

If, for example, the opposing party's discovery demands would require a broader litigation hold than the corporation thinks is mandated by the needs of the case, corporations should consider filing a motion for protective order and requesting the court's assistance in limiting the scope of the litigation hold to one that is proportional to the needs of the case. The alternative is to risk sanctions for failing to implement a litigation hold plan in a timely manner. Similarly, there may be limited circumstances where implementing an appropriate litigation hold will be unduly burdensome or expensive "considering the amount in controversy, the importance of the issues at stake in the action, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." *See* proposed amendment to Fed. R. Civ. Proc. 26(b)(1), available at http://www.uscourts.gov/file/document/congress-materials. If those limited circumstances are present, corporations should consider moving the court for a protective order to limit the scope of the hold. In such situations, however, the corporation must still be able to identify the key custodians and data sources that would be included within the scope of the proposed, more narrow litigation hold.

The proposed amendments to the Federal Rules of Civil Procedure will also impact the sanctions that will be available if electronically stored information (ESI) is destroyed. In theory, under the proposed amendment to Rule 37, it will be more difficult for corporations to be sanctioned for the unintentional destruction of data. Rather, the proposed amendment to Rule 37(e) states that sanctions are only triggered if a party fails to take reasonable steps to preserve ESI that cannot be restored or otherwise replaced. Even then, if the court finds that a party was prejudiced by the loss of the ESI, the court may only "order measures no greater than necessary to cure the prejudice." *See* Proposed Amendment to Rule 37(e)(1), available at http://www.uscourts.gov/file/document/congress-materials. The court may order an adverse inference against the party that destroyed the ESI, or order dismissal of the action or entry of default judgment, only upon a finding that the party "acted with the intent to deprive another party of the information's use in the litigation." *See* Proposed Amendment to Rule 37(e)(2), available at http://www.uscourts.gov/file/document/congress-materials.

Conclusion

The implementation of an effective litigation hold plan is a group effort. All eyes will be on your client's "reasonable steps" to preserve information beginning December 1, 2015. Outside counsel should make sure they are intimately involved in all aspects of the process and that the corporation has involved the necessary departments, identified key custodians, and halted the automatic destruction of data. Outside counsel must also make sure to follow up with the corporation on a regular basis to confirm that the hold remains in effect. Further, in-house counsel should ensure their outside counsel is kept in the loop and that the litigation hold plan does not devolve into a ministerial corporate function that may become prone to error. Finally, the corporation should document its global processes and procedures for its litigation hold plan, as well as its execution of the litigation hold plan for individual cases, because written, repeatable processes will keep your corporation out of trouble more often than not.