Former Employees – Gone, But Not (Digitally) Forgotten

August, 2014

Employee turnover is a reality faced by all organizations. In 2013, the annual turnover rate in the United States, including both voluntary and involuntary employee departures, averaged 13 percent across all industries, according to the Society for Human Resource Management’s (SHRM) Human Capital Benchmarking Database. In addition, according to the most recent survey conducted by PayScale, more than half of all Fortune 500 companies experience a median employee tenure of 3.7 years or less. For some industries, such as information technology (IT), the median employee tenure is as low as 1.1 years.

In addition to the challenges employee turnover creates for the traditional business divisions of companies — including increased recruitment and training costs, decreased and/or inconsistent productivity, low morale, and weakened customer relationships — employee turnover can present a unique set of risks for corporate legal and IT departments charged with managing their organization’s compliance with data preservation obligations.

Former Employees and the Duty to Preserve Relevant Information

It is well established that once a lawsuit or investigation has commenced or is reasonably foreseeable, a party has a duty to preserve information within its custody and control, including electronically stored information (ESI), that may be relevant to the litigation or potential litigation. At the outset of a legal action, parties have an obligation to identify and issue a legal hold to “key players” and other employees determined to have access to potentially relevant information, as well as to take active steps to ensure that all relevant data for those individuals is preserved during the pendency of the lawsuit.

Changes in employment status do not diminish an organization’s preservation duties. Key players can therefore include former employees as well as employees who depart from the company following commencement of a legal action and issuance of a legal hold notice. Indeed, with the typical lawsuit and investigation spanning, on average, two to three years, it is not uncommon for identified key players to depart a company during the pendency of an action. Nevertheless, once a duty to preserve attaches, failure to adequately preserve relevant information — including the records of former employees, within the party’s possession, custody or control — can expose a party and its counsel to significant penalties for spoliation of evidence, including monetary sanctions, cost-shifting, adverse inference jury instructions, preclusion of evidence, professional discipline, and the entry of default judgment or dismissal.

Employee Departures and Spoliation Risk

Employee departures can threaten a company’s ability to comply with ongoing preservation obligations, and often bring increased risks of spoliation arising from the unintentional destruction or loss of data that can occur at the time of departure. These risks frequently emerge due to the inconsistent, and often conflicting, objectives of the company’s IT and legal departments. When an employee is terminated, resigns or transfers departments, it is customary for IT to swiftly collect the departing employee’s equipment as well as delete his or her existing email and local/network stored files, so the equipment can be reissued to another user and server space can be freed up for other employees. In carrying out this routine practice, organizations often fail to inform their legal department and/or properly address the risk of inadvertent deletion or modification of former employee information subject to preservation requirements. As a result, relevant ESI that a party is required to preserve is frequently destroyed or altered, leaving the company exposed to potential spoliation sanctions.

The Threat of Sanctions

Courts are not reluctant to impose sanctions on parties who fail to meet their preservation obligations with respect to former employee ESI. In a Title VII action alleging racial discrimination and retaliatory discharge, the court in Knickerbocker v. Corinthian Colleges awarded plaintiffs $25,000 along with attorneys’ fees as a result of defendant’s deletion of two former employees’ email files after its duty to preserve was triggered. In that case, the email files of the two former employees were destroyed pursuant to an automated process whereby departed employee email accounts were automatically deleted 30 days following receipt of a standard termination notice from the HR department. The court found that defendant’s preservation
duty attached at the time it received EEOC notices for the two employees, just days following the issuance of the employees’ termination notices but before the automatic deletion occurred. As a result, the court concluded that defendant’s failure to suspend its email system’s standard process of automatically deleting departed employee email accounts constituted a violation of its duty to preserve relevant data, representing an act of willful spoliation and meriting sanctions.

Cache La Poudre Feeds, LLC v. Land O’Lakes, Inc. involved a trademark infringement claim in which plaintiff alleged that defendant was unlawfully using a protected mark for animal feed products that had been used by plaintiff for more than 10 years. Plaintiff brought a motion seeking sanctions for destruction of evidence, citing defendant’s alleged failure to suspend routine deletion protocols for several employees who departed subsequent to commencement of the lawsuit. Siding with plaintiff’s position, the court ultimately found these actions to constitute spoliation warranting monetary sanctions of $5,000 for defendant’s transgressions. Specifically, the court found that defendant’s continued practice of wiping and reissuing hard drives of former key player employees (without preserving the deleted data) following commencement of the lawsuit violated defendant’s obligation to preserve evidence in that case.

Reaching Out to Former Employees

The courts appear to be divided when it comes to a company’s obligation to contact former employees to assist in satisfying preservation obligations. As a general rule, a company is required to preserve only what is found within its possession, custody or control, and most courts are unwilling to require an investigation that extends beyond current employees and company-controlled data sources. Still, a number of courts have taken the opposite position, finding that preservation obligations require a party to contact former employees to assist in the identification of potentially relevant information. This may include reaching out to former employees to determine whether they are in possession of responsive documents requiring preservation. Indeed, in certain circumstances, courts have found a company’s duty to preserve to extend to the personal email files and personal devices of former employees.

Suggested Best Practices

The above cases highlight the various risks encountered by organizations as they navigate their ongoing preservation obligations in the face of employee turnover. The following are suggested best practices offered to assist in mitigating these risks.

Immediate Capture

In most cases, the departure of an employee whose data is subject to legal hold requirements should trigger the immediate imaging of that individual's hard drive(s) and other relevant data sources, to be preserved during the pendency of the litigation.

If policy requires the imaging of former employee hard drives following departure, accurate records identifying the source and content of all former employee preserved data should be maintained. Companies should also accurately track the return and final disposition of company-owned equipment, including any reuse or reissuance of equipment to new users.

In the case of an involuntary dismissal of an employee whose data is subject to a legal hold, it may be prudent to make a backup copy of the employee’s data prior to termination, to ensure data is not inadvertently or intentionally deleted or altered prior to departure.

Restricting Access

At the time of departure, companies should take immediate steps to revoke former employee access to all company-controlled hardware and applications, to prevent accidental or intentional modification or deletion of ESI subject to ongoing preservation requirements.

Sound Information Governance

In practice, it is wise for organizations to establish and follow a comprehensive information governance program that includes data retention policies specifically designed to address former employee data. These policies should include rules as well as methods and timelines for preserving former employee data following departure, and should address all employee-accessed data sources (including nontraditional sources, such as mobile devices, cloud-based storage and social media).

Separate rules should apply to former employees whose data is subject to ongoing preservation obligations. At a minimum, policies requiring the automatic destruction of employee data following departure should be suspended for employees who are subject to ongoing preservation requirements.
To foreclose ambiguities regarding what falls within a company’s possession, custody or control, organizations should consider establishing and enforcing rules that preclude employees from using personal email accounts to transact company business.

Interdepartmental Coordination of Legal Hold Activities

Organizations should consider establishing processes to coordinate the activities of their legal, HR and IT departments once litigation commences. At a minimum, the legal department should be informed immediately of any changes in the employment status of employees subject to an open legal hold, before data is inadvertently destroyed or altered via routine IT activities. Once informed, counsel should communicate directly with employees prior to departure to confirm compliance with preservation requirements as well as to personally oversee preservation activities.

Organizations should maintain lists of employees who are subject to open legal holds and should periodically review those lists to track departing employees to ensure their data is accounted for, as well as to track employees who might have inherited data from departed employees.

Using ESI Interviews to Address Former Employee ESI

During the initial stages of litigation, it is customary for counsel to conduct ESI interviews with key players and the company’s IT department in order to identify sources of potentially relevant information subject to preservation. When interviewing key players, counsel should ask questions about former employees who might have created or stored information potentially relevant to the matter. Similarly, in its discussions with IT, counsel should ask targeted questions about how former employee equipment and data is routinely handled by the organization following departure, including when and how such data is preserved, along with the location, ease of accessibility and period of retention of preserved data.

Managing Preservation through the Exit Interview

A company’s standard exit interview process should include questions relating to the departing employee’s adherence to ongoing data preservation obligations, along with any known spoliation issues. In addition, departing employees should be asked whether they used personal email or personal storage devices (e.g., thumb drives, mobile devices, tablets) during the course of their employment to store company ESI that is subject to a legal hold.

Company-related information determined to be in the possession, custody or control of the departing employee should be returned to the company at the time of the interview. This is particularly important for companies that allow employees to use personal devices, such as smart phones and tablets, to conduct company business (BYOD), as these devices will be departing along with the employee. Companies allowing BYOD might consider including in their formal use policies specific language allowing for the physical inspection and/or imaging of such devices by corporate IT prior to departure.

Departing employees should be asked to document all sources of data subject to open legal holds, as well as to affirm in writing that all information subject to open holds is within the possession, custody and control of the company, and that no such information exists on the employee’s personal devices or in personal email accounts.

Conclusion

An organization’s legal obligations reach far beyond its proverbial digital line of sight. While IT and legal departments continue to increase their awareness of the preservation obligations imposed by federal and local state rules, they frequently fail to adequately address the special risks associated with employee departures, leaving their organizations exposed to sanctions. Although no company can control the inevitability or timing of employee turnover, by institutionalizing awareness and protective measures through proactive, standardized practices, organizations can significantly reduce the spoliation risks associated with employee departures.

Authors:

Jeffrey Teso
Managing Director
+202 670-2120

Andy Gandhi
Managing Director
+212 763-9749

For More Information:
Global Forensic and Dispute Services


[3] Id.


[8] Id. at *8-*9.

[9] Id. at *26-*27.

[10] Id. at *27.


[12] Id. at 637.

[13] Id. at 629.

[14] Id. at 627.


-----------------------------------------------------------------------------------------------------------------------------------------------------------

Professional Spotlight

Michael Conner
Managing Director
San Francisco

Specializing in electronic discovery, database analytics and forensic acquisition, Michael has more than 18 years of experience in the collection, processing and production of electronically stored information (ESI).

Read more.