

# The Legal Intelligencer

## Departing Employee Preservation Program: Understanding Potential Pitfalls



By Tara Lawler and William Childress

Data that is potentially responsive and must be preserved and eventually collected and produced in an active litigation is typically tied to individual employees who are custodians of the data. If an employee leaves the company tomorrow, what will happen to the data controlled by the employee?

*L-R: William Childress and Tara Lawler of Morgan Lewis & Bockius. Courtesy photos*

March 5, 2023

Companies are dealing with more uncertainty around the management of company data than ever before. The recent move to remote workforces, the proliferation of technology being used by employees to store company data and now the potential—or reality—of large numbers of employees exiting companies are creating a risk of data loss. In particular, departing employees, whether they leave a company voluntarily or involuntarily, present additional risk to an organization when those employees are subject to ongoing preservation obligations for active litigations or investigations.

After years of volatility in the labor market, it is important that companies plan for employee departures and manage departures to reduce the risk of data loss. In this article, we offer guidance on how companies should approach the dilemma that employee departures present when the departing employee is subject to an active legal hold and key steps to take to develop a defensible departing employee preservation program.

At the start of the pandemic, companies faced unprecedented challenges with their workforces. In short order, many companies had to transform to fully remote work environments. In other instances, companies had to downsize rapidly to survive widespread lockdowns. By April 2020, the unemployment rate had quadrupled from pre-pandemic levels.

However, the pendulum swung quickly toward full employment. As the unemployment rate declined, employee “quit rates” set modern records. Observers have dubbed this trend of voluntary departures as the “Great Resignation.” The U.S. Bureau of Labor Statistics shows that approximately 50 million people left their jobs in 2022. Voluntary quit rates may subside this year, but involuntary ones could quickly spike. Now, as the shadow of a recession looms over the economy, large-scale layoffs in the tech and finance sectors have made headlines.

Data that is potentially responsive and must be preserved and eventually collected and produced in an active litigation is typically tied to individual employees who are custodians of the data. If an employee leaves the company tomorrow, what will happen to the data controlled by the employee? Every organization should know the answer to this question and have a thorough plan in place to handle departing employee data that is subject to legal hold.

### **Key Steps to Develop a Successful Departing Employee Preservation Program**

A company should take the following steps to implement a program to identify departing employees who are subject to an active legal hold(s) and to ensure any data subject to an ongoing preservation obligation is properly identified and tracked.

#### **Identify the Owner of the Program and Key Stakeholders**

Several departments will need to be involved in the creation and implementation of the departing employee preservation program including IT, human resources (HR), privacy, if a global company, the legal department and the e-discovery team, if one exists. The legal department and e-discovery team should own the process and ensure that all stakeholders are aware of the program and sent periodic reminders and updates regarding changes to the program, as needed. This will be an iterative process as

data systems and other policies may change over time. It is important that the program is periodically reviewed for required updates or changes, and that proper implementation is confirmed as effective. Applicable policies and procedures should spell out what happens when an employee leaves the company and who bears responsibility to ensure proper preservation.

### **Identify Who Is Departing the Company and Whether They Are Under Legal Hold**

This step of the process relies on custodial tracking and management as part of the company's overall legal hold and HR process. HR is central to the success of a departing employee program. HR departments are often the hub of employee offboarding and notifications regarding when a departure is occurring and this information should be shared by HR with key stakeholders. When an employee is subject to a legal hold, an exit can become more complicated, and tracking departures is critical. Assessment of legal holds should occur as soon an employee exit is processed. If HR keeps information about a departure in a silo, then important data may be lost.

The legal or e-discovery team will need visibility into the list of active holds that the departing employee may be subject to and to reconfirm that the custodial data is still needed for the active matter as well as the scope of data sources required to be preserved. Therefore, there must also be a mechanism in place wherein HR notifies the legal department of an upcoming departure.

For companies with automated legal hold tools and advanced HR systems, the systems should be synched so that notifications about a departure are automated and the legal hold tool flags whether the departing employee is subject to one or more legal holds. For companies that do not have a central legal hold tracking tool or state of the art HR systems, tracking can be more complicated. To effectively track an exit, a manual determination will need to be made whether an employee leaving the company is under a legal hold and a protocol put in place to ensure that HR and Legal are exchanging this key information.

It is also imperative that if the departing employee has a successor who will assume possession of potentially responsive data, that that employee is added to the legal hold. Therefore, the tracking system should have a means to detect successors as part of the exit process.

## **Understand Custodial Data Sources and Notify Appropriate IT Personnel of the Exit**

Key to a successful departing employee preservation program is understanding the company's IT landscape. This step, in some part, has likely already been accomplished as part of a standard legal hold program in that custodians are instructed on where and how to preserve data in their possession that is subject to a legal hold. This program and knowledge of data sources is central to establishing an effective departing employee program.

To build an effective exit process, there must be a clear understanding of when data will expire and what events trigger disposition of data and in particular, former employee data. Managing employee exits should be built around these deadlines. In other words, how long will devices, email, and other personal accounts be retained after an employee leaves? Mailbox and OneDrive may go into a soft delete status after an employee's last day and become unrecoverable after a short period (30 or 60 days). Will an employee's computer and mobile devices be wiped immediately upon return, placed on a shelf for a set period of time, or will they automatically be imaged? Consideration should be given to whether the company has any process in place to make computers and other electronic devices inoperative if they are not returned by a certain date. Some company IT departments may issue "kill pills" to the devices of departed employees. This can be a necessary protective measure for data security considerations, especially when dealing with remote workers, but there should be a means to override its application for devices subject to legal hold.

It is important to be aware of any retention functions and to have a general understanding of data stewards—the individuals typically in charge of the systems, assets and purge functions. The data stewards and other IT stakeholders will need to receive notice of departures and to timely suspend, if needed, any of the purge functions on a departing employee's data who is subject to an active hold. Technology aids can assist with consistency and effectiveness. The IT stakeholders are presumably already kept apprised of existing legal holds and involved in the implementation of the holds. As such, IT can be a vital resource in the successful implementation of a departing employee preservation program in that IT may know before the legal department that an employee on legal hold is departing the company. IT personnel should be instructed to confirm whether an employee was on hold when

departing (and before wiping employee devices or allowing auto purge functions to progress) as a best practice to ensure potentially relevant data is preserved.

Companies should ensure their processes are designed to capture holds placed on former employees before any of their data is permanently lost. As discussed above, an employee's departure will often trigger automatic deletion functions. Companies should have a means to detect these types of situations and intervene to stop automatic deletions, where data is still recoverable once a hold is placed on a former employee.

### **Use Exit Interviews to Facilitate Data Preservation**

Typically, HR or management conducts an exit Interview with the departing employee. An exit interview is a wrap-up meeting between the company and the departing employee and is a tool through which legal hold related questions can be built in. The exit interview can be a means by which the company reminds the departing employee of his or her existing and on-going preservation obligations and determine if potentially responsive data needs to be preserved. Interviews can help the legal team gather key information such as the types of potentially relevant data, where the data resides, and what the custodian knows about the matter. This information will assist the legal team in making informed decisions in the future, when the custodian is not readily available.

Where possible, the legal team managing the legal hold should also attempt to interview the exiting custodian. This is especially true for any high-stake matters or for key custodians. Exit interviews should also attempt to address key data sources that are controlled by the custodian. This includes mobile devices, paper records, and portable media. Although IT can act to prevent disposition of certain custodial data, data sources controlled exclusively by individual employees are more complicated to preserve because they require cooperation and proactivity.

Exit interviews, however, are not always feasible. Employee departures are complicated because there is no uniform departure period. Voluntary departures depend entirely on the individual providing notice. Although a two-week notice period is standard in the United States, notices can be shorter. Another complicating factor is that an employee's "last day" of employment and "last day worked" can vary.

Employees may use weeks of vacation immediately prior to leaving their positions, making themselves essentially unavailable to assist in preservation efforts. Outside of the United States, “garden leave” can precede a termination by several months.

For layoffs, although the company determines the exit date, due to the sensitivity of such matters, information may not be shared in a timely manner with the individuals who need to work on preservation of data. Companies should also be aware that large reductions in force can put a strain on preservation efforts and should always include data preservation in the planning process. Mergers and corporate spinoffs can also lead to numerous employee “departures” at the same time, straining HR, IT and legal hold teams.

As such, if an exit interview cannot be completed, the company should consider including in exiting documentation reminders about his or her legal hold obligations. An employee’s final days in a position can be hectic, and it is a best practice to send a reminder on how the employee should handle data and devices when offboarding. For simplicity, some legal departments may develop standing directives to retain all the data of departing employees, including imaging devices or preserving devices in place. However, this type of preservation will lead to an over accumulation of data as long as the legal hold remains in place. When issuing legal holds, including questionnaires for custodians to complete about their data sources and storage locations can assist in managing custodian departures. As a related point, because employee attrition rates are historically high, legal departments should promptly place employees under legal hold.

### **Other Considerations**

- **Mobile data preservation can be complicated**

Under the best of circumstances, mobile data collections are difficult endeavors. Adding in the urgency created by a custodian’s departure can amplify this problem. Exit interviews and custodial data questionnaires can inform whether mobile preservation is needed. Keep it simple. If no unique, potentially relevant data exists on a mobile device, then there is no need to preserve mobile data. When mobile data needs to be preserved as part of an exit, companies need to plan carefully.

As discussed above, mobile devices are typically controlled by the employee, not IT. Therefore, the ability to access the mobile data may require custodian cooperation, if the collection occurs before the exit. If a company device cannot be collected before the employee leaves, then steps should be taken to ensure passcodes and passwords are collected as part of the exit interview. Unless the company has the means to bypass passcodes, this information will be needed to access the device, and without it, the mobile device can turn into a paperweight. Also, keep in mind that custodians can easily and quickly wipe mobile devices by using factory reset settings. Therefore, it is important to remind custodians under legal hold not to reset company phones before returning them.

Personal devices operating under BYOD programs are even thornier to manage. Companies should confirm their BYOD policies are up to date and are consistent with their legal hold and IG policies. If potentially relevant, unique data is on an employee's personal phone, act quickly, especially if the legal matter is in a jurisdiction that considers such devices under the employer's custody or control. As explained above, most departures come with short notice periods so there is a small window to collect such data. Departing employees may also resist collections from their personal devices and company leverage over them can be quite limited. If there is no time to complete a forensic collection before the employee's last day, have them provide screenshots of the relevant messages and assess whether the data is actually needed for the hold. If the mobile data is needed for hold, secure the employee's commitment to cooperate in the collection at a future date, and document everything to show reasonable preservation efforts. Also, keep in mind that an employee leaving involuntarily may be less cooperative, especially when collection from a personal device is requested.

- **Departing employees located outside the United States**

Global organizations should be aware that employees under U.S. legal holds can be located in countries with strict privacy laws. Companies should know what local laws impact the collection, transfer, and storage of data related to departing employees who are subject to active legal holds. Does the data need to be preserved in country? If not, is there a means to transfer and store the data in the United States or another country? Attorneys managing legal holds should consider these questions when

placing custodians outside the United States under a legal hold and plan ahead. Privacy concerns weigh in favor of properly scoping and narrowly tailoring legal holds.

- **The remote worker dilemma**

Prior to the pandemic, most employees spent their last day in the office. This in-person presence facilitated device return, exit interviews, and the collection of other information necessary for data retention. Now, remote employment is ubiquitous. Therefore, companies must plan to offboard remotely. Key to this is ensuring employees are instructed to promptly return devices and given the means to do so, including pre-paid shipping options for those not located near an office. Further, device returns should be tracked. Whether this responsibility is assigned to HR or the employee's manager or to IT, someone must ensure employee devices are returned. If devices are not returned promptly, companies must have a means to follow up with employees. All returned devices should be tracked and checked to confirm whether their last assigned user was under a legal hold. No devices should be reassigned or wiped without first assessing whether they are under a legal hold.

The bottom line:

Departing employees, whether they leave a company voluntarily or involuntarily, present a unique risk to every organization. The potential for the loss of data is real. Companies should plan for employee exits and build a program aimed at preserving data that the company needs to preserve for an active litigation. Although numerous factors make this process complicated, understanding potential pitfalls and advanced planning will help mitigate the risk of data loss.

*Morgan, Lewis & Bockius partner Tara Lawler's practice focuses on e-discovery, information management and data privacy. Senior attorney William Childress counsels clients on electronic discovery at the firm.*

*Reprinted with permission from the March 5, 2023 issue of The Legal Intelligencer © 2023 ALM Media Properties, LLC. Further duplication without permission is prohibited. All rights reserved.*