Discontinue remote electronic access — The traditional office is no longer confined to the walls surrounding an employee’s desk. Employees access their computers and voicemail from remote locations. It is important to immediately discontinue a departing employee’s electronic access. Doing so can bolster an employer’s ability to seek trade secret protection for its information, and it can limit the ability of a former employee to electronically misappropriate key information.

Ensure return of records and property — Departing employees, particularly long time employees, may have acquired company records in hard or electronic form over a period of years. Employers are well advised to seek written confirmation from departing employees that all such records and information obtained as a result of their employment with the company have been returned, including company information that may reside on electronic devices owned by the employee. Return of all office keys, building access cards, and tangible property should also be required.

Freeze usage of employee’s computer — When an employee resigns, it is not always possible to know immediately whether the employee presents an unfair competitive threat. It may be a few weeks before an employer learns that the former employee engaged in misconduct. Computers previously used by the former employee can be a valuable tool when conducting an after-the-fact investigation, but key evidence can be lost (e.g., overwritten or deleted) if the employer has continued to use the former employee’s computer. For this reason, a former employee’s computer should be removed from active use if there is any suspicion that a former employee poses a competitive threat. If this is not feasible, making a forensic image of the computer presents another alternative.

Exit interview — If the departing employee is willing, the employer should conduct an exit interview during which the employee is asked about future employment plans, reminded of contractual obligations, and requested to return all property of the employer.

Check computers — Employees often plan departures months in advance. Key files and information can be emailed to a private e-mail address or downloaded to a flash drive with the stroke of a few buttons. Unusual emails or bulk transfers can provide an employer with an indication that departing employees may not have the best of intentions.

Transition clients — Clients should be assigned new company contacts as soon as possible. This will enhance the employer’s chances of solidifying and maintaining the client relationship, and may uncover evidence of the former employee’s misconduct.

Interview co-workers — Departing employees often talk to their co-workers. In these discussions, they may foreshadow their post-employment intentions, reveal prior misconduct, or perhaps they may attempt to recruit co-workers for the benefit of their new employers. Co-workers can be a valuable source of information for the investigating former employer.

Online social media — If a former employee’s misconduct or candor is in question, former employers might consider reviewing statements made by former employees on online social media. These outlets are sometimes used by departing employees to contact former clients or to post confidential information.

Notify former employee of contractual obligations — Departing employees should be reminded immediately in writing of any contractual obligations they may have (e.g., non-competition and non-disclosure agreements), advised that the employer takes these obligations seriously, and provided a written copy of their agreements.

Scan files — A former employee’s files should be reviewed to determine whether anything appears to be missing or destroyed.