KRONENBERGER | ROSENFELD

CRISIS RESPONSE CHECKLIST

What to Do After Key Employee Announces Departure

By taking quick action after a key employee announces he or she is leaving for a competitor, you can significantly limit the chances that your trade secrets will end up at your competitor. So, when you learn that an employee is leaving, consider taking the following actions:

- [ ] 1. Lock-Out Departing Employee from All Key Systems
- [ ] 2. Seize Control of Computers
- [ ] 3. Preserve Log Data
- [ ] 4. Analyze Log Data for Recent Access to Sensitive Data
- [ ] 5. Confirm Confidentiality in Writing with Departing Employee
- [ ] 6. Inquire about Departing Employee's New Job
- [ ] 7. Reminder Correspondence to Departing Employee
- [ ] 8. Put New Employer On Notice
- [ ] 9. Monitor the Situation

What Not to Do

Often when key employees leave, they also leave passwords to personal email and social media accounts cached in browsers on company-owned computers. This would give an employer the capability to log in to these accounts for the purpose of investigating whether the former employee is misappropriating trade secrets. Employers should know that using an employee's or former employee's passwords to gain access to personal email accounts (Gmail, Yahoo, etc.) or social media accounts (Facebook, LinkedIn) is unlawful under both state and federal laws. Furthermore, reviewing stored communications in such personal accounts is also unlawful. In fact, there are criminal penalties associated with this sort of unauthorized access to accounts and unauthorized review of stored communications. Thus, while tempting, employers should not log into any of these accounts or otherwise review any personal stored communications of the current or former employee.

KRONENBERGER | ROSENFELD

CRISIS RESPONSE CHECKLIST

1. Lock-Out Departing Employee from All Key Systems

This may seem obvious, but inexplicable delays do sometimes occur. The policy should be an immediate lock-out.

2. Seize Control of Computers

Immediately obtain control of all laptops and other computers used by the departing employee. These devices could have been used to access trade secrets or other sensitive data. And, they might contain important evidence of plans to steal trade secrets.

3. Preserve Log Data

If your firm has created logging systems within its network, and on employee computers, preserve all such logs (showing access to trade secrets, or saving data to USB or cloud drives). This is especially true for any logs that are automatically written over periodically due to large file sizes.

4. Analyze Log Data for Recent Access to Sensitive Data

After the key logging data is preserved, analyze the data for suspicious activity. For example, the departing employee may have had lawful access to a particular database on a daily basis. But, if say, the departing employee exported the entire database to an external or cloud drive, this would be highly suspicious. Look for any evidence of an employee emailing sensitive documents to their personal, non-employer email addresses. This includes any emails that may have been sent and then deleted from a sent-mail folder.

5. Confirm Confidentiality in Writing with Departing Employee

Confirm in writing that the employee knows that certain types of information are trade secrets. If the employee refuses to sign a document acknowledging the scope of trade secrets, the document should be handed or emailed back to the employee. The goal is to eliminate any argument that the departing employee does not know what information is a trade secret protected under previously signed confidentiality agreement(s).

6. Inquire about Departing Employee's New Job

Obtain the name of the new employer and the employee's job title. This provides an easy way to determine if there's a risk of trade secret misappropriation. For instance, it would perhaps be inevitable for the departing employee to refrain from using the trade secrets if its an identical job title and position at a competing company.

7. Reminder Correspondence to Departing Employee

After the employee leaves, send a reminder letter to the former employee that trade secrets cannot be shared with the new employer. And, from the time the employee gives notice to the time they start the new position, you might discover new information about potential trade secret misappropriation. Include this new information in follow-up correspondence.

8. Put New Employer On Notice

Inform the new employer of potential trade secret misappropriation before the employee starts the job. This puts the new employer on notice of any potential liability associated with misappropriation - even it's inadvertent. This eliminates the argument that the new employer didn't know the new employee might misappropriate trade secrets.

9. Monitor the Situation

Perhaps the hardest thing to do is just to sit back and monitor the situation looking for evidence of misappropriation. This is especially difficult when a former key employee has left. It's not uncommon for ex-employees to stay in touch with their former co-workers, third party marketing partners, and vendors. These are excellent sources to report on potential misappropriation. And of course, you might discover forensic evidence of misappropriation. At that point, seek legal guidance from counsel who has dealt with trade secret issues with departing employees to discuss next steps.