CONTRIBUTED CONTENT & PRESENTATIONS

Before The Dust Settles: Immediate Actions You Should Take When Your Secrets Are Compromised

MARCH 24, 2020

Authors: Alyssa A. Moscarino

Endless days. Sleepless nights. Time. Money. Worry. You have spent a career building up your company and expanding your business. Then, one otherwise unassuming afternoon, you learn that a disgruntled employee or envious competitor has compromised your trade secrets. The secret sauce that you spent years (even decades) developing. Panic can lead to inaction. And inaction can lead to irreparable harm. There are things that you can and should do in those precious moments to protect yourself and enhance the potential outcome

The law broadly defines what constitutes a "trade secret." In the transportation and logistics space, your secrets may include customer lists (both current and prospective), marketing methods and strategies, pricing information and rates, market intelligence, training materials, business processes, and proprietary technology solutions. The highly competitive and fragmented nature of this industry means that these secrets can have extraordinary importance for the continued success of your business. As a result, you should be taking all necessary steps to guard these secrets jealously.

Something Is Wrong. What Do I Do Now?

The following "Response Checklist" will help mitigate negative consequences that stem from a trade secret breach. These consequences may include a delayed incident response, increased costs, litigation, shareholder derivative lawsuits, loss of business, and reputational harm. Moreover, in the event litigation ensues, jurors are keenly interested in a company's efforts to mitigate loss; in other words, jurors want to know that a company did not sit on its hands after it learned that its information had been compromised.

Technology has changed the playing field. And savvy business professionals know that within the hard drives and smartphones, and in the cloud, you will find the evidence necessary to stop the theft or win in court.

Here are some strategies and steps that you can include in your trade secret protection action plan in real time.

- Immediately suspend suspect employee access to trade secret information.
    - Examples of this include changing passcodes, collecting employee access cards or flash drives, denying access to clean rooms, temporarily locking employees out of their company computers, seizing company-issued smartphones, and denying access to the company's physical office.

- Assemble your team.
  - Alert and involve human resources employees and direct them to assemble personnel files of suspected individuals, including the latest versions of confidentiality, non-disclosure, noncompetition, and other agreements.
  - Instruct your information technology team to preserve all relevant information and conduct a forensic review of electronically stored information. If you do not have in-house information technology folks (or ones that are forensic experts), consider hiring a third-party vendor.

- Appoint a trusted individual (perhaps a human resources officer or high-level director) to conduct employee interviews.
  - This process should be an effort to identify all individuals who had access to the stolen information to ultimately find the root of the breach.
  - Collect witness statements during the interviews.
  - Consider involving an attorney to shield the interviews from later discovery as privileged.

- Consider all former employees, consultants, business partners, or the like who had access to trade secret information within the past two years.
  - Identify where each individual works now, including whether for or with a competitor.
  - Identify whether such individuals were terminated, denied a promotion, or any other circumstances that would lead to resentment.

- Apprehend company property from those with suspected involvement in the breach (company smartphones, laptops, iPads, etc.).
  - This is an uncomfortable, albeit necessary step. Consulting legal counsel to develop policies that clearly state what is and is not company property is prudent. Remember, it is your property.

- Have your IT department or a third-party vendor standing by to forensically image the collected devices.
  - While smartphones and laptops are the most obvious devices, consider nontraditional electronic data sources as well. These may include employee security cards, parking garage logs, machine hard drives, and surveillance camera footage.
  - Do not resume an employee's access to trade secret information unless said employee has been cleared.

- Document your response.

    - This will include recording all response actions, such as suspending and strengthening passwords, logging company property apprehended and searched, collecting and maintaining signed and written witness statements gathered during the interviews, etc. If litigation is needed, your documentation will be critical.

- Consult legal counsel to determine whether your jurisdiction has any applicable laws or regulations that govern how to respond to such an incident.
    - This is a vitally important step to place your company in the best position should litigation become necessary to protect your secret sauce.
    - Your legal counsel can work with you to enforce your rights. This might include drafting reminder letters to employees of their obligations, cease and desist or other notice letters indicating knowledge of the breach, and ultimately litigation and appropriate remedies, such as a temporary restraining order or preliminary injunction.

For more information, please contact Matthew D. Gurbach or Alyssa A. Moscarino.

Matthew D. Gurbach is Co-Chair of Benesch's Products Liability practice and can be reached at mgurbach@beneschlaw.com or (216) 363-4413.

Alyssa A. Moscarino is an associate in Benesch's Litigation Practice Group and can be reached at amoscarino@beneschlaw.com or (216) 338-7939.