FORENSIC SERVICES

TRADE SECRET AND DEPARTED EMPLOYEE

SullivanStrickler

OVERVIEW

Every newly hired employee is both a potential asset and a potential liability to an employer.

In a scenario when an employee is in the process of moving between two companies. This employee is focused on all the attributes and assets being brought to the new company, but there should be awareness of the liabilities as well.

The current employment contract, employee handbook and trade secret law are full of potential pitfalls that need to be addressed before the transition.

There are default obligations, generic obligations and contractual obligations related to the former employer's trade secrets. Failure to meet contractural obligations can bring a law suit or loss of employment. In addition to engineering and product design information the former employer might consider customer lists, customer contact information, marketing information, pricing schedules, proposals, all trade secrets or confidential materials. Business emails are another source of potential prior employer's property.

We recommend engagement with a labor and employment lawyer with litigation experience to review past employment and confidentiality agreements. Having a lawyer review and interpret prior employer's employee handbook is critical during this transition. Together, a well-documented defensible way of handling data that keeps any potential liability from attaching itself to you as you transition can be determined. The lawyer will advise if the previous employer's property, including electronic data, contractually must be returned to the former employer upon termination or separation.

SCENARIO 1

Problem Faced

An employee recently left, and the employer is suspicious intellectual property was taken.

Solution Offered

SullivanStrickler will image the employee's computer as well as get a copy of his mailbox, cellphone (if available) and other devices.

Once the devices are imaged, we provide a set of triage reports which provide communications (such as text messages) from the cellphones, USB connectivity analysis, file explorer artifact analysis, and a list of office documents that were opened by the user. We also look for use of cloud services like Dropbox, Google Drive or OneDrive.

If the above analysis finds indications of IP theft, it is typically sufficient to get a judge to order a further round of discovery focused on the personal devices and new employer devices. We can and do assist in those levels of discovery as well.

SCENARIO 2

Problem Faced

The new employer has been contacted by a previous employer with allegations of IP theft.

Solution Offered

There is no prescribed typical response that SullivanStrickler can bring to bear. We would work with the client to either

1. Formulate a response, or
2. Have the court name SullivanStrickler a neutral expert and assigned specific duties.

A list of recent cases and a curriculum vitae of our head of forensics can be provided as reference.

SCENARIO 3

Problem Faced

A new employee has been hired, but they have not yet started in the role.

Solution Offered

We offer proactive “defensible deletion" services to work with the new employee to ensure that the former employer's IP has been removed from the personal devices and cloud accounts. This is a proactive service deployed with every newly hired employee in order to avoid a future lawsuit. If there is a lawsuit, it greatly increases the likelihood of a summary judgement on the part of the hiring firm with minimal litigation cost.

The process begins with outside counsel reviewing past employment and confidentiality agreements with the potential new hire. They note if the previous employer’s trade secrets contractually must be returned to the former employer upon termination, etc. They discuss the possibility that the employee might have confidential or trade secrets of his former employer in his or her possession.

Once the outside counsel understands the prior obligations of the soon to be hired employee, they consult and advise that a “defensible deletion” protocol is deployed. The “defensible deletion” protocol may include imaging the personal devices and cloud accounts, then exporting out copies of the former employer's materials for return, deleting the materials from the personal devices and cloud accounts, and finally re-imaging.

In general, our clients prefer to have this process implemented and completed before the new hire’s first day of working. That is an effort to ensure there is no window of time offending materials might get transferred into their enterprise.