UNIVERSITY OF TEXAS SCHOOL OF LAW CLE
Essential Non-Compete and Trade Secret Law: A Practical Guide to Talent Management

Presented:

Dallas, Texas – September 9, 2016
Houston, Texas – October 7, 2016

INVESTIGATING THE EMPLOYEE DEPARTURE:
Practical Tips for Protecting Against and Mitigating Data Asset Loss

Presented by
Laura M. Merritt

Laura M. Merritt
Boulette Golden & Marin L.L.P.
2801 Via Fortuna, Suite 530
Austin, TX 78746

laura@boulettegolden.com
512.732.8903

TABLE OF CONTENTS

I. INTRODUCTION

Employee departures carry with them many potential landmines and difficulties for the now-former employer, from talent drain, workflow disruption, and lowering of morale among remaining employees, to more direct hits like employee theft and use of confidential information. This paper and presentation focus on practical tips to help protect "assets on the move," whether those assets be human or data-based, and protection of assets begins with a plan.

II. POLICY AND PROCESS SOLUTIONS: PEOPLE, PLANS AND PROBLEMS

As in most efforts, failing to plan for employee departures is equivalent to planning to fail. Other papers and speakers in this course have addressed the importance and how-to of critical employment agreements such as restrictive covenants and confidentiality agreements, as well as litigation tactics such as the injunctive process. A common thread in protecting a company when any employee departs is laying the proper documentary early-stage groundwork.

Putting together a comprehensive and coordinated data protection plan begins not after HR receives an employee's resignation notice, but before that employee is ever hired. In addition to the crucial agreements discussed in other papers and presentations, a company should protect its data by implementing electronic systems and confidential information policies and procedures, training employees and managers on those policies, considering the use of transition and/or severance agreements to ensure good behavior from resigning employees, and implementing coordinated human resources, legal and IT department processes that kick in when an employee separation occurs.

To address the security risks raised in a workforce, an employer should consider: (1) what information needs to be protected; (2) who needs access to that information; and (3) what steps should be taken within the company's particular workforce dynamic to protect both inadvertent and intentional disclosure of that information.

The first step is to identify the universe of information mobile workers will be able to access but that the company is attempting to protect. Information such as customer lists, pricing information, client

information, customer preferences, buyer contracts, market strategies, blueprints and drawings have all been afforded trade secret status.

For example, a mobile or remote worker with mobile and off-site access to company data, creates not only a high risk of misappropriation, theft, or improper use of company trade secrets and proprietary and confidential information (because it becomes easier to abscond with company information), but it also creates a greater risk that courts will not deem information worthy of protection if the company cannot show that it took "reasonable efforts" to keep its secrets secret. Given that a mobile workforce will, by definition, take a company's secrets outside the company's walls,[1] it is especially important that a company using such a workforce take steps to protect its confidential information *before* the employees and the data leave the building. Otherwise, the company risks both the actual disclosure of its information and its legal ability to protect the information in court.

Once a company has identified the information it seeks to protect, access to it should be limited to only those employees who need to have access in order to perform their job. As other papers and presentations have noted, a key factor in the analysis of whether a company took reasonable measures to protect its secrets is whether the company limited access to the information to a subset of its employees.

A. Electronic Systems and Data Protection Policies

[1] There are numerous trade secret cases where the company secret is kept literally under lock and key in a vault or other secured, physical location. *In Re Bass*, 113 S.W.3d 735, 742 (Tex. 2003) ("The data were kept in a secured, climate regulated vault that was accessible only to those who knew the combination."); *In re XTO Res. I, LP*, 248 S.W.3d 898, 902 (Tex.App.-Fort Worth 2008, no pet.) ("the data were kept in a vault accessible only to those who knew the combination, and employees needed a security card just to enter the work area"); *IAC, Ltd. v. Bell Helicopter Textron, Inc.*, 160 S.W.3d 191, 198 (Tex.App.-Fort Worth 2005, no pet.) ("Bell showed that it guards the secrecy of its data by storing the originals of its drawings and specifications in a vault, posting security guards at its plants, requiring persons entering the plant to identify themselves and wear identification badges, checking material going in and out of the plant, limiting access to data on its internal computer system to persons with appropriate system identification and passwords.").

Title search: Investigating the Employee Departure: Practical Tips for Protecting Against and Mitigating Data Asset Loss

First appeared as part of the conference materials for the
2016 Essential Non-Compete and Trade Secret Law: A Practical Guide to Talent Management session
"Investigating the Employee Departure"