BFV

BERMAN FINK VAN HORN

ATTORNEYS AT LAW

Keep Your Competitive Edge & Protect Your Practice from Unfair Competition and Trade Secret Theft

Presented By:

Neal F. Weinrich

Berman Fink Van Horn P.C.

nweinrich@bfvlaw.com

www.bfvlaw.com

Goals of Presentation

- How to Protect the Practice When Employees Leave
  - What can you do proactively?
  - What do you do when an employee leaves and may be competing unfairly?

- How to Protect the Practice When Hiring Employees

How to Protect Your Practice From Departing Employees

- What Worries You When an Employee Leaves?

What Worries You When an Employee Leaves?

- Have they talked to other employees?
- Are they taking other employees with them?
- Will other employees follow them?
- Are they going to work for a competitor?
- Have they said anything to patients?
- Are they going to solicit patients?
- Have they taken any information?

How to Protect Your Practice From Departing Employees

- How to Stop or Reduce the Worrying
  - What Should You Be Doing in the Regular Course of Business?
  - What Do you Do When Someone Leaves?

What Should You Be Doing?

- Use Good Agreements
  - Noncompetes
  - Customer Nonsolicits
  - Employee Nonrecruitment Covenants
  - Nondisclosure covenants
  - Return of property
  - Computer use provisions
  - IP Ownership
- Review Your Agreements Regularly

What Should You Be Doing?

- Draft and implement policies.
    - Email usage policy
    - Device/computer usage policy

- Train on the policies.

- Create a culture of protection of confidential information and trade secrets.

What are Trade Secrets?

- Financial, business, scientific, technical, economic or engineering information, including a formula, pattern, plan, code, compilation, program device, design, prototype, method, technique, process or procedure, that:
  - Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by the public; and
  - Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Economic Espionage Act and Defend Trade Secrets Act, 18 U.S.C. §1831.

What are Trade Secrets?

- Financial information
- Scientific information
- Technical information
- Economic Information
- Engineering information
- Patterns
- Plans
- Compilations
- Formulas
- Designs
- Prototypes
- Methods
- Techniques
- Processes
- Procedures
- Codes
- Patient List
- Customer lists
- Referral Source Lists/Data
- Programs

What is “Confidential Information”

- Data or information:
  - (A) Relating to the business of the employer, regardless of whether the data or information constitutes a trade secret as that term is defined in Article 1 of Chapter 10 of Title 10
  - (B) Disclosed to the employee or of which the employee became aware of as a consequence of the employee's relationship with the employer;
  - (C) Having value to the employer;
  - (D) Not generally known to competitors of the employer; and
  - (E) Which includes trade secrets, methods of operation, names of customers, price lists, financial information and projections, route books, personnel data, and similar information
    - *O.C.G.A. § 13-8-51(3)*

What is “Confidential Information”?

- Does NOT include data or information:
  - (A) which has been voluntarily disclosed to the public by the employer, except where such public disclosure has been made by the employee without authorization from the employer;
  - (B) which has been independently developed and disclosed by others; or
  - (C) which has otherwise entered the public domain through lawful means.

O.C.G.A. § 13-8-51(3)

Who is Stealing Your Information?

- More common than you think
  - 2013 survey showed that approximately half of the respondents said they have taken data.
  - Of these, 40% planned to use it in their new jobs.

    -- Study by Symantec and the Ponemon Institute

  - Number of cases overseen by FBI increased by > 60% between 2009 and 2013

How is Information Stolen So Readily?

- More technology creates greater opportunity
  - Smartphones, tablets and laptops
  - Portable drives
  - Cloud storage
- Hard to find and stop
- As technology develops, litigation increases
  - Litigation has doubled nearly every decade in past 30 years

Remedies

- Defend Trade Secrets Act.
- Georgia Trade Secrets Act.
- Georgia Computer Systems Protection Act
- Contractual Remedies

- Under the Georgia Trade Secrets Act and the federal Defend Trade Secrets Act, information only constitutes a trade secret if it “is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

What do You do to Make these Remedies Available?

Keys to an Effective Information Protection Strategy

- Understand the threat
- Identify and inventory competitive information
- Conduct a trade secret audit
- Develop a trade secret protection plan
- Keep pace with technology/prepare for vulnerabilities

Keys to an Effective Protection Strategy

Identify and Inventory

- An inventory allows you to better ensure your company's competitive information is considered a trade secret.
- Determine what confidential information, processes, or other data give the company a competitive advantage.

Keys to an Effective Protection Strategy

Develop a trade secret protection plan

- In writing
- Segregate trade secrets to be treated differently than other information
  - Necessary to prove the information constitutes trade secrets if legal action is required after a theft
  - Allows protective measures to be narrowly targeted
- Follow the Plan

Keys to an Effective Protection Strategy

Limited, Need-to-Know Access

- Specifically identify who can access information, only as needed to perform job
- Prevent unauthorized persons from performing certain actions (save, copy, print, modify, delete)
- Track who accesses information: who, when, duration, action
- Store in a separate location
- Electronic information management systems

Keys to an Effective Protection Strategy

Marking

- Label trade secret materials, both electronically and in hard copy
  - *For example*: “TRADE SECRET. Confidential and/or proprietary property of [Company]. Do not copy or circulate.”
  - Pop-up marking: user of a company’s server must acknowledge and reaffirm that they are accessing confidential information/trade secrets
  - Digital labels to track materials issued to specific individuals

Keys to an Effective Protection Strategy

Agreements

Acknowledgements

- Minimize loss of trade secrets due to ignorance, carelessness
- Employee manual: discuss trade secret protection plan, employees' obligations, potential consequences.
  - Written acknowledgement: that employees read and understand manual and plan. First day of employment. Store safely.
  - Entrance interviews to explain responsibility not to disclose *other companies'* and *your company's* trade secrets and confidential information.
  - Remind employees during annual reviews, employee meetings.
  - Exit interviews and termination certificates

Keys to an Effective Protection Strategy

Training and Culture

- Create a culture that respects confidential information;
- Conduct training on importance of and methods for protecting confidential information;
- Document training efforts (with sign-in sheet).

Keys to an Effective Protection Strategy

Physical Security

- Facility Security
  - Store and lock hard copies, laptops, other storage tools (e.g., disks).
  - Security guards, visitor logs, cameras

- Restricted access: Track and limit access to building and trade secret areas through access codes or keycards.

Keys to an Effective Protection Strategy

IT Infrastructure/Protected Networks

- Network Security: Encryption, access controls, traffic monitoring, security software, separate servers or hard drives.
- Device Security: Passwords, encryption, wiping or shut off capabilities, locks.
- All passwords complex and periodically changed.
- Public computers: Prohibit access of company networks, trade secrets, confidential information

Keys to an Effective Protection Strategy

Exit Interviews

- Remind employees of non-disclosure obligations
- Ask direct questions:
  - Do you have hard copies of information at home?
  - Are you in possession of a storage device that contains company information?
  - Have you ever sent company emails to a personal email address?
  - In anticipation of leaving have you downloaded any information?

What Do You Do When Someone Leaves?

- An employee is leaving and there is fear he or she may compete unfairly – what do you do?
- Assess the Risk
    - What was their role?
    - What information did they have access to?
    - What are the circumstances surrounding their departure?
    - What are their future plans?
    - Is there any suspicious activity?
- Is Further Investigation or Legal Guidance Needed?

What Do You Do When Someone Leaves?

- Do a Thorough Exit Interview
- Go over the Departing Employee's Agreement with the Employee
- Investigate to Determine if any Information Has Been Taken
    - Email
    - Computer Analysis
    - Other Electronic Activity
- Once a Risk Assessment is Complete, Evaluate What Additional Steps Are Needed

What to Do When You Are Hiring from a Competitor

- What's the Goal? To Avoid Exposing the Practice to Liability

- How Do You Accomplish that? By Being Circumspect in Your Hiring Practices

Hiring Considerations and Steps

- Request copies of a candidate's agreements.
    - Get the agreements early in the process.
- Tell candidates you expect them to comply with their legal and enforceable contractual obligations to their current employer
    - Fiduciary obligations
    - Notice provisions
- Remind candidates of their obligation not to take confidential information or trade secrets of their current employer.
    - Verbally
    - In Writing (offer letter; employment agreement).
- Discuss expectations with respect to communications with patients.
- Discuss expectations with respect to communications with employees.

Conclusion

Thank You

BFV

BERMAN FINK VAN HORN

ATTORNEYS AT LAW

Neal F. Weinrich

Email: nweinrich@bfvlaw.com

Phone: 404.681.6016

bfvlaw.com


Allianz