Bloomberg BNA

BNA's
Corporate Counsel Weekly™

Competitor Lift-Outs: Protecting Your Firm In Pursuing and Avoiding Litigation for Employee Raiding

BY HARRY S. DAVIS AND CHRISTOPHER H. GIAMPAPA

When a competitor hires multiple employees from your business or, worse, persuades an entire team or business unit to defect to a competitor, the resulting harm may be severe. Along with substantial lost revenues and profits, the consequences can include the risk of additional employee defections, decreased morale, reputational harm and the loss of key clients, trade secrets and confidential information. Successful competitor lift-outs may even, in extreme cases, threaten the target firm's viability. Financial services and technology firms, among others, frequently face the threat of this kind of lift-out by a competitor, often referred to as employee raiding, pirating or poaching. In this evolving area of law, what strategies can firms use to protect themselves from an employee lift-out by a rival firm? How can firms best position themselves for litigation if a competitor engages in employee raiding? This article answers these questions as well as how a firm that intends to hire a number of employees from a competitor can best position itself for litigation.

Sound Defense Starts Long Before a Raid Occurs

Before a raid occurs, thoughtful and enforceable protections should be put in place through employment contracts, particularly for important producers and key supervisory personnel. One common measure is to prohibit employees from competing against their employer during the term of their contracts and for a reasonable period of time after the contract expires. Of course, such non-competition provisions are more likely to be enforced by courts where the employer agrees to pay the employees for the period they sit out of the marketplace (garden leave), and where the restrictions are appropriately limited in geographic reach and time. Thoughtfully tailored non-competition restrictions that take into account the employee's seniority, role and importance may make it easier for an employer to persuade a tribunal that a restrictive covenant is necessary to protect the employer's business and are more likely to be enforceable in litigation following a raid than boilerplate provisions seeking to restrict differently situated employees through uniform terms without accounting for their individual role and responsibilities.

Anti-solicitation provisions restricting employees from soliciting the same customers with whom the employees did business are also common, but whether a particular customer was ''solicited'' or instead approached the employee at a new place of business may be difficult to prove in litigation. As a result, the better practice is to contractually prohibit employees from accepting or doing business with the employee's former customers or from steering or inducing customers to do business with any other person except their employer for a reasonable period following separation. Provisions like this may give management time to take action to try to key customers even when key employees leave. Likewise, employers should consider broad anti-poaching provisions in their employment contracts, prohibiting employees from hiring, attempting to hire, soliciting or recruiting other employees to accept employment (or be retained as a consultant) by any other firm for a reasonable period following the employee's separation from your business.

Businesses should also consider requiring employees who are approached or solicited by a competitor for employment to provide notice to the company's senior management of the approach or employment offer. Where employees adhere to such provisions, employers gain a valuable opportunity to counter-offer or to seek to retain other key staff. If only one or a handful of employees who are approached by a competitor provides notice, that is often enough for management to determine which teams are vulnerable or are already ''in play.'' Even where the notice provision is not honored by employees who wish to keep their impending move a secret, proof of a breach of

Harry S. Davis, a litigation partner, and Christopher H. Giampapa, a litigation special counsel, practice complex commercial litigation at Schulte Roth & Zabel LLP and recently concluded a four-month jury trial involving an 80-employee lift-out between competitors.

 ISSN 0886-0475

contract (or claims for inducing a breach or interfering with an employment contract) for failing to provide notice are easier to prove than many other claims; further, successfully establishing the ''easier'' breach of contract claims can help you prove the more difficult ones. Employees who have plainly breached one duty or contractual provision may be more likely to be perceived by the judge or jury as having breached other contractual provisions or common law obligations. And when many employees leave having failed to comply with a simple and straight-forward notice provision and all join the same rival firm, a trier of fact may be more likely to conclude that the employees breached their contracts at the urging of the rival firm.

Sound anti-raiding defenses also include thoughtfully drafted confidentiality provisions in employment contracts, confidentiality agreements and policies such as employee handbooks. Employers should try to define carefully and specifically what information is to be kept confidential, rather than using vague or general language. For example, employers should explicitly identify, as appropriate, financial models, trading software, source or object code as part of what constitutes confidential and proprietary information in employment contracts. Likewise, employers that wish to treat the amount of revenue produced by individual employees or the compensation paid to individual employees as confidential should explicitly define confidential information to include that information, while carving out the employee's right to disclose his or her own salary and compensation information. Careful thought in advance about what information the employer considers confidential, backed up by documented steps to restrict access to and secure that information, makes it easier to litigate both injunctive relief and damages following a raid by a rival firm.

In advance of a raid, employers will also be well served to set clear policies concerning the employer's right to access electronic information on company computers and company supplied or supported laptops, cell phones and other mobile devices, including information accessed through web browsers. Employers should state that they have the right to access, inspect, and copy any communications, including voicemails and text messages, on devices connected to or supported by the company's IT infrastructure and that employees have no expectation of privacy in such information. Those policies will prove valuable when a company seeks an injunction (or damages) in response to a lift-out.

Companies will also need to ensure that their practices live up to their written policies. For example, writing into your policies and contracts that employees are required to return all firm-issued laptops will not help if your firm typically ignores those contractual requirements and lets employees take their firm laptops with them. And it compounds the problem if you are going to let employees take their laptops without first wiping them clean of the firm's confidential information. Not only does failing to adhere to your own confidentiality policies make it more likely that departing employees will leave with your firm's confidential information, it will make it more difficult for you to demonstrate to a court that you actually had effective procedures in place to ensure confidentiality over information that you later might claim has been misappropriated by a departing employee or a competitor. Policies are great but they are no substitute for effective enforcement and ensuring that your firm's practices accord with your written policies and employee handbooks.

Perhaps most importantly, sound contracts and thoughtful policies are no substitute for carefully managing talent with an eye towards employee satisfaction. Keeping key employees happy is often the best preventative medicine to protect your firm. Inevitably, though, some employees are less than satisfied. Where major producers or business unit leaders are plainly unhappy, businesses should consider proactive monitoring, consistent with written policies and privacy laws, to permit business leaders to detect and intervene in the event that key personnel decide to shop a significant part of the business to a competitor.

Taking Action After a Raid

When a company learns a competitor is raiding its business, obtaining information about what personnel or business units are ''in play'' is critical. Such information often comes in piecemeal fashion, from employees who have been contacted by a rival or by a company insider about jumping ship. Quickly investigating and interviewing employees can help uncover the extent of the problem, thereby putting management in the best position to focus on retention (and if necessary, replacements) in key areas. Your competitor may have been planning the raid for weeks or months and so may have a substantial head start on you. Although your firm may be in crisis mode with many different tasks to accomplish, there is no substitute for a timely, well-thought out response.

Rapid and early investigation into available electronic evidence is also advisable. Crucial, but potentially ephemeral electronic evidence can often be obtained in the days and weeks following a raid, but if the evidence cannot be used due to privacy restrictions or the inability to access it rapidly, a significant advantage can be lost. Mobile devices can also contain valuable, time-stamped location data that can be used to prove who was involved in coordinating a lift-out, and when and where they did so. (For iPhone users interested in seeing how powerful such sources of evidence can be, go to Settings / Privacy / Location Services, then ''Frequent Locations'' to see a map of your most frequent locations. Many users are often unaware that such data is, by default, being automatically collected.)

Once the hiring firm has been identified, cease and desist letters, written reminders to departing employees about their contractual and legal obligations, including the obligations to protect company trade secrets and confidential information, are common next steps, often with the assistance of outside counsel. It is also important to adhere to established exit procedures to ensure the return of company issued laptops, storage devices and cell phones in the wake of a raid. Likewise, the early retention of a computer forensics firm may be quite valuable in preserving valuable computer forensic evidence and also in understanding—and later proving—how and why the lift-out occurred. Firms may also be able to pinpoint instances where a departing employee copied confidential information on the way out of the door, or tried to destroy evidence of his or her copying, both of which can prove invaluable in the litigation that may follow a raid. When a raid is suspected or is in process, companies should also take steps to consider and preserve all sources of potentially relevant evidence. In addition to email,

  CCW ISSN 0886-0475

documents on hard drives, instant messages, text messages and the like, that may also include other less frequently considered sources like keycard or ID badge swipes, photocopier use, internet histories and access to or downloads from sensitive files or servers.

Lawsuits seeking injunctive relief and/or damages, both against the hiring rival and, where appropriate, against disloyal employees, are often necessary. In general, the common laws of most states do not recognize a cause of action for raiding *per se*. Instead, claims for employee lift-outs are commonly brought against rivals using existing torts such as unfair competition, misappropriation of trade secrets or confidential information, tortious interference or inducing breaches of contract or common law duties. Claims against disloyal employees may include some of those same torts, but also often include claims for breach of contract, breach of fiduciary duty and breach of the duty of loyalty. Financial services businesses for which FINRA arbitration is often mandatory should note that FINRA does recognize a cause of action for raiding.[1] Thus, where FINRA arbitration is mandatory, a claim for raiding is commonly brought along with other common law torts.

Because a raided company may pursue a claim for damages against a competitor and/or former employees, it is important to avoid making statements in the aftermath of the raid that will impair the company's ability to obtain damages. That may mean resisting the understandable pressure to assure investors and customers that the company has ''recovered,'' that its business will continue ''uninterrupted'' or to downplay the importance of the departures for the company's revenues, profits or future prospects. Companies that may seek damages should be circumspect not only in their public statements, but also in their private communications with the media, analysts and other audiences.

Companies seeking to recover from a raid should also approach hiring or acquiring replacements with an eye towards how the company's own hiring conduct will be viewed in subsequent litigation. Don't lightly sacrifice the ability to go to court or another tribunal while wearing a white hat. While it can be tempting to decide that the ''gloves are coming off'' and to resort to the same hiring tactics by which one was recently victimized, doing so can undermine an otherwise successful case for substantial damages. (At a minimum, it is difficult to sue your competitor for lifting out your company's Chicago office if your company just hired the employees of the rival's Boston office. Similarly, it is hard to claim that your desks' or offices' revenue production is confidential if you routinely request that information from employees of your rivals when you are considering employing them.) Jurors, judges and arbitrators are sensitive to perceived hypocrisy or double standards, and a company's own aggressive hiring tactics to recover from a raid can readily be turned against the firm by means of an unclean hands defense or an argument that certain hiring practices that you are challenging as illegal or unfair competition are common place or accepted in a particular industry, since your firm uses the same hiring practices, which you are now criticizing.

Strategies for Hiring From Competitors

When looking to fill needs by hiring from a competitor, what are some strategies companies should use to avoid becoming embroiled in litigation or to minimize exposure if they are sued?

First, approach hiring teams with the prospect of litigation firmly in mind. This typically means hiring from a competitor in stages and understanding the obligations that prospective employees may owe to their current employer. Although hiring firms may want to approach business unit leaders first, make sure that discussions with those individuals are limited to discussions about hiring that person and don't stray into discussions about how to hire team members. And hiring firms should certainly do their own recruiting: don't use a rival's business leader to recruit his or her subordinates at the competitor. Understand the potential hires' employment agreements and make sure that you understand their non-compete clauses and other contractual restrictions, including post-termination restrictions. (In reviewing existing contracts between a prospective employee and a rival, it is often advisable for the employee's personal lawyer to redact arguably confidential information from the contracts before they are sent to you for review. While it is essential to understand a potential employee's contract term and post-termination restrictions, contract provisions relating to salary, bonuses or other arguably confidential information should be avoided.) After assessing the potential employee's obligations to his or her current or previous employer, wait for the employee to clear post-termination restrictions before allowing that employee to assist recruiting efforts.

Second, when negotiating with business leaders from a rival firm, set clear expectations. Explain the company does not want to receive confidential information or trade secrets from, or documents from, the rival. Make a record of refusing to accept a rival's confidential information or documents if they are offered.

Third, instruct the prospective employees not to talk to others at his or her current employer about the opportunity to join a new firm while they are still employed or subject to post-termination restrictions. Also consider instructing the new hires to advise their current employer promptly, regardless of their current contractual obligations; transparency by employees about an impending move may help tip the balance of the equities and convince a trier of fact that the hiring was not intended to sandbag or harm the competitor.

Fourth, consider obtaining a representation in the new hire's employment contract that the individual did not bring with him or her (or provide the new employer with) any documents or confidential information from the prior employer. Trust but verify. Where a lawsuit is likely or pending, promptly gather electronic evidence concerning activities of the recently hired employees during the recruiting process. To the extent there is potential liability for recruiting co-workers or investors before joining the new employer or, for taking a rival's business information or trade secrets, early detection is important for understanding and minimizing potential exposure.

Savvy employees will often ask for indemnification from the new firm in the event they are sued by their former employer. Although providing both individual counsel and indemnification are common place in many industries, carefully consider the scope of the indemnity and how it

[1] See, e.g., *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Morgan Stanley & Co.*, 2010 NASD Arb. LEXIS 1236 (Nov. 23, 2010).

will be perceived in any subsequent litigation. For example, an indemnity provision that protects a former employee for sharing confidential documents or information from the prior employer may later be viewed by the judge or jury as a red flag proving that your firm knew that the new employee was taking confidential information from his or her prior employer, or even that your firm is to blame for that theft.

Likewise, it is important to be cautious in public statements about the hiring. While it may be tempting to publicize a major hiring at the expense of a competitor (or to gloat), resist the temptation to do so. Expressing an intent to ''hit the competition where it hurts'' or to ''destroy'' a rival may help an adversary support a claim for unfair competition or other business torts.[2] Similarly, while competitive hyperbole like, ''when we are done, there is going to be nothing left at XYZ firm'' or ''you better join us because we are hiring all the top producers at your firm and you don't want to be the last one standing when the firm collapses'' may help in your recruiting efforts, statements like these can be devastating in subsequent litigation as evidencing an intent to harm or destroy a rival.

In short, careful planning in advance of a rival's hiring campaign can give businesses a leg up in subsequent litigation. Businesses looking to avoid or respond to employee raiding, or those looking to make substantial hires from rivals, are well advised to consult with experienced counsel for advice about the particulars of their industry and situation.

[2] See, e.g., *The Finish Line, Inc. v. Foot Locker, Inc.*, 2006 BL 7710, at *9 (S.D. Ind. 2006).

  CCW ISSN 0886-0475