

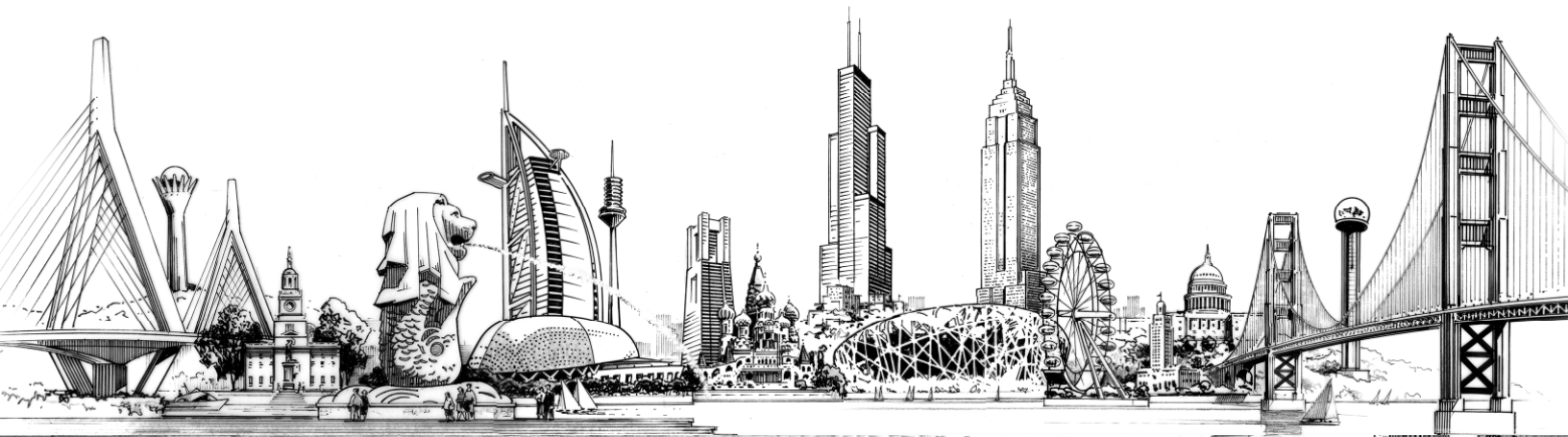
Morgan Lewis

ニューヨーク日本商工会議所

**JAPANESE CHAMBER OF COMMERCE AND
INDUSTRY OF NEW YORK, INC.**

知らないと怖い・2015年米国雇用法の落とし穴

2015: PITFALLS IN US EMPLOYMENT LAW THAT YOU NEED TO KNOW



Morgan Lewis

table of contents

| | tab |
|---|----------|
| 知らないと怖い・2015年米国雇用法の落とし穴 2015: Pitfalls in US Employment Law That You Need to Know | 1 |
| 賃金および労働時間に関連する問題を防止する方法: トップ 10 Top 10 Ways to Avoid Wage and Hour Trouble | 2 |
| 内部告発者関連法の遵守チェックリスト Whistleblower Compliance Checklist | 3 |
| 貴社の最も貴重な資産と競争力の危機? Are Your Company's Most Valuable Assets and Competitive Advantage at Risk? | 4 |

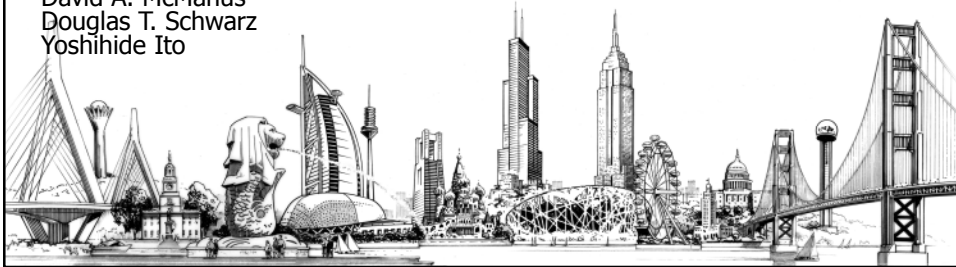
Tab 1

Morgan Lewis

**2015: PITFALLS IN US EMPLOYMENT
LAW THAT YOU NEED TO KNOW**

Japanese Chamber of Commerce and Industry of New York, Inc.
February 26, 2015

David A. McManus
Douglas T. Schwarz
Yoshihide Ito

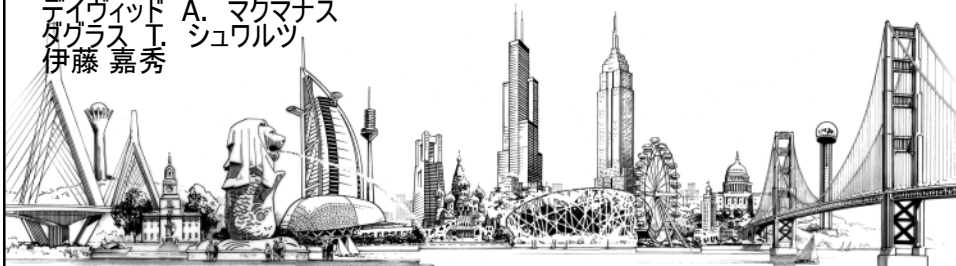


Morgan Lewis

**知らないと怖い・
2015年米国雇用法の落とし穴**

ニューヨーク日本商工会議所
2015年2月26日

デイヴィッド A. マクマナス
ダグラス T. シュワルツ
伊藤 嘉秀



2015 Overview

- Trends in 2015
- Major Concerns for Companies with US Operations
- Special Issues for Japanese Corporations
 - Responding to changing workforce demographics
 - Greater diversity in management

Morgan Lewis

3

2015年の概観

- 2015年に見られる傾向
- 米国でビジネス活動に従事する企業にとっての主要な懸念事項
- 日本企業に特有の問題点
 - 変化する労働人口構成への対応
 - ダイバーシティ・マネジメントの広まり

Morgan Lewis

4

2015 Pitfalls

- Significant Wage and Hour Risks
- Whistleblower Retaliation
- Cyber Security and Social Media in the Workplace
- Responding to High-Stakes, High-Visibility Employment Litigation

Morgan Lewis

5

2015年の落とし穴

- 賃金と労働時間に関する顕著なリスク
- 内部告発者に対する報復行為
- 職場におけるサイバーセキュリティおよびソーシャルメディアへの対応
- リスクと注目度の高い訴訟への対応

Morgan Lewis

6

Morgan Lewis

Significant Wage and Hour Risks

© 2015 Morgan, Lewis & Bockius LLP

Morgan Lewis

賃金と労働時間に関する顕著なリスク

© 2015 Morgan, Lewis & Bockius LLP

Wage and Hour – Large Awards

Workers reach \$21 million settlement against [REDACTED]
LA Times, May 14, 2014

[REDACTED] will settle with unpaid interns for \$6.4M,
Syracuse Post Standard, October 24, 2014

More Workers Are Claiming Wage Theft, *New York Times*,
August 31, 2014

Strip clubs that denied dancers 'legal wages' agree to \$4.3M
payout, *New York Post*, October 7, 2014

Morgan

Give me a break . . . or \$56.5 Million!, *Asian Journal*, August 16, 2014

賃金および労働時間 高額な和解金額

[REDACTED] が従業員と 2,100万ドルで和解、
LA Times, May 14, 2014

[REDACTED]、賃金支給を行わなかったインターンと640
万ドルで和解、*Syracuse Post Standard*, October 24, 2014

賃金窃盗を訴える従業員の増加、*New York Times*, August 31, 2014

ダンサーに「法定賃金」の支払いを拒否したストリップ・ク
ラブ、430万ドルの支払に同意、*New York Post*, October 7, 2014

Morgan

いい加減にしろ... さもなければ、5,650万ドル支払え!、
Asian Journal, August 16, 2014

Wage and Hour Issues

- Typical Allegations:
 - Employee Misclassification
 - Exempt vs. Nonexempt
 - Independent Contractor Status
 - Off-the-Clock Work
 - Use of Company Devices (iPhone, BlackBerry, etc.)
 - Donning and Doffing
 - Inaccurate Time-Keeping Practices
 - Travel/Commute Time
 - Intern Claims
 - Meal and Rest Periods (where legally mandated)

Morgan Lewis

11

賃金および労働時間問題

- 典型的な訴え:
 - 従業員の誤分類
 - エグゼンプト 対 ノンエグゼンプト
 - 契約社員・独立契約者
 - 勤務時間外の業務
 - 会社のデバイスの使用 (アイフォン、ブラックベリー等)
 - (安全用具などの) 着脱 (Donning & Doffing)
 - 不適切な勤務時間記録の慣行
 - 出張・通勤時間
 - インターンからの苦情
 - 食事・休憩時間の割り当て (法的に義務付けられている場合)

Morgan Lewis

12

Wage and Hour Risk Mitigation Strategies

- Conduct privileged audits of employee classification (exempt, nonexempt, independent contractor, etc.) and pay practices (timing of payment, calculation of overtime, rounding, etc.)
- Ensure that company policies require employees to record all work time and make clear that all hours worked will be paid (including unauthorized overtime)
- Review compliance with state and local law (e.g., meal and rest period requirements, payment upon termination rules, required postings, etc.)
- Train HR, payroll, and management employees
- Consider arbitration agreements

Morgan Lewis

13

賃金および労働時間 リスク軽減のための戦略

- 従業員の分類（エグゼンプト、ノンエグゼンプト、契約社員・独立契約者等）および賃金支給の慣行（支給時期、超過勤務手当の計算、端数処理方法等）について、秘匿特権下の監査を行う
- 従業員が実際に勤務した全ての時間を記録し（無許可の残業も含む）、そのような時間の全てについて賃金が支払われることが会社の方針として義務付けられているかについて確認する
- 州および地方の法律へのコンプライアンスの見直し（食事・休憩時間に関する義務、解雇時支給の規則、法令揭示の義務等）
- HR、給与管理、経営部署に所属する従業員向けの研修
- 仲裁合意書の検討

Morgan Lewis

14

Morgan Lewis

Whistleblower Retaliation

© 2015 Morgan, Lewis & Bockius LLP

Morgan Lewis

内部告発者への報復行為

© 2015 Morgan, Lewis & Bockius LLP

Whistleblower Retaliation Large Awards

██████████ OKs paying surgeon \$10 million in whistleblower-retaliation case, *LA Times*, April 22, 2014

SEC accuses firm of whistleblower retaliation, *USA Today*, June 16, 2014

██████████ Whistleblower Files Another Lawsuit, *Wall Street Journal*, October 3, 2014

Morgan L Whistleblowers Reporting to Middle Managers First, Showing Need For Training, *Wall Street Journal*, October 13, 2014

内部告発者への報復行為 高額な和解金

内部告発者への報復事件で ██████████ が外科医に対して1,000万ドルの支払いを認める、*LA Times*, April 22, 2014

SECが内部告発者に対する報復行為で会社を告発、*USA Today*, June 16, 2014

██████████ の内部告発者による更なる訴訟案件の提起、*Wall Street Journal*, October 3, 2014

Morgan L 内部告発者はまず、中間管理職に報告するので、研修が必要、*Wall Street Journal*, October 13, 2014

Whistleblower Retaliation Issues

- Origins of whistleblower retaliation claims:
 - Reports regarding potential violations of law, FINRA rules, reporting obligations, or internal controls relating to SEC rules and regulations
 - Allegations of unlawful sales practices; health and safety violations; discrimination or harassment
 - Challenges to accounting, bookkeeping, and recording practices
 - Reports regarding potential violations of the employer's corporate compliance, code of conduct, or ethics program
 - Mail or wire fraud

Morgan Lewis

19

内部告発者への報復行為に関連する問題

- 内部告発者への報復行為クレーム発生のきっかけとなるもの
 - 法律、FINRA規則、報告義務、またはSECの規則および規制に関する内部管理の潜在的な違反についての報告
 - 違法な販売慣習の疑い、健康・安全規則の違反、差別またはハラスメント
 - 経理、帳簿、記録に関する慣行への批判
 - 雇用主のコーポレート・コンプライアンス、行動規範、または倫理制度の潜在的な違反に関する報告
 - 郵便あるいは電子通信手段による詐欺

Morgan Lewis

20

Whistleblower Retaliation Risk Mitigation Strategies

- Ensure that underlying accounting practices, reporting procedures, and other policies comply with the law
- Conduct and document prompt, appropriate investigations of employee complaints
- Define “whistleblower” status broadly when considering whether employee engaged in protected activity
 - Internal and external reports of misconduct
 - Written or verbal reports
- Consider the protected status of an employee before taking any adverse employment action
- Consider the protected status of an employee who takes confidential documents or information

Morgan Lewis

21

内部告発者への報復行為 リスク軽減のための戦略

- 基礎的な経理の慣行、報告手続き、その他の制度が法令に従っていることを確認する
- 従業員からの苦情に対しては、迅速かつ適切に調査を行い、文書として記録を保存する
- 従業員の行為が保護の対象となるか否かを判断する場合、「内部告発者」の立場を広範に定義する
 - 違法行為の内部および外部への報告
 - 文書または口頭での報告
- 雇用上、悪影響を及ぼす措置を取る前に、保護の対象となる者か考慮する
- 機密文書あるいは情報を持ち出す従業員が、保護の対象となる者か考慮する

Morgan Lewis

22

Morgan Lewis

Cyber Security and Social Media
in the Workplace

© 2015 Morgan, Lewis & Bockius LLP

Morgan Lewis

職場におけるサイバーセキュリティー
およびソーシャルメディアの使用

© 2015 Morgan, Lewis & Bockius LLP

Cyber Security

- Cyber Security Risks
 - Significant data breaches
 - Disclosure of confidential information and trade secrets
 - Grave damage to corporate reputation
 - Costly disclosures and significant risk of litigation
- Risk Mitigation Strategies
 - Confidentiality and Nondisclosure Agreements with employees who have access to sensitive information
 - Policies regarding passwords, security of company devices and personal devices containing company information, etc.
 - Employee training regarding data protection

Morgan Lewis

25

サイバーセキュリティ

- サイバーセキュリティに関連するリスク
 - 大量データの流出
 - 機密情報および営業秘密 (trade secrets) の暴露
 - 企業の評判に深刻なダメージ
 - 暴露対策費用と高い訴訟リスク
- リスク軽減のための戦略
 - 機密情報を扱う従業員と秘密保持合意書 (Confidentiality and Non-Disclosure Agreements) を締結する
 - パスワード、企業情報を搭載した会社用または私用デバイスのセキュリティ
 - データ保護に関する従業員向け研修

Morgan Lewis

26

Use of Social Media

- Risks of Social Media in the Workplace
 - Disclosure of confidential company information
 - Workplace bullying, harassment, and intimidation
 - Forum for protected concerted activity
- Risk Mitigation Strategies
 - State clear policy for use of social media at work
 - Clarify that employees have no expectation of privacy with respect to use of social media at work
 - Establish clear rules regarding confidential information
 - Clarify when employees may speak on behalf of company
 - Monitor and enforce the social media policy

Morgan Lewis

27

ソーシャルメディアの使用

- 職場におけるソーシャルメディアのリスク
 - 企業の機密情報の開示
 - 職場でのいじめ、ハラスメント、威圧的言動
 - 法的保護の対象となる共同行為・活動の場
- リスク軽減のための戦略
 - 職場でのソーシャルメディアの使用に関する明確な方針の確立
 - 職場でのソーシャルメディアの使用に際しては、一般に従業員のプライバシーは保護されないことを明示
 - 機密情報に関する明確な規則を作成
 - 従業員が企業に代わって意見を述べることのできる状況の特定
 - ソーシャルメディアポリシーの監視と執行

Morgan Lewis

28

Morgan Lewis

Responding to High-Stakes,
High-Visibility Employment Litigation

© 2015 Morgan, Lewis & Bockius LLP

Morgan Lewis

リスクと注目度の高い雇用関連訴訟への対応

© 2015 Morgan, Lewis & Bockius LLP

Responding to High-Stakes, High-Visibility Employment Litigation

- Identify legal team (typically a combination of in-house and external counsel)
- Identify key witnesses, decisionmakers, and document custodians
- Issue preservation notice
- Evaluate your IT and data security systems—implement appropriate protocols
- Consider retaining public relations firm
- Identify company spokesperson, if needed

Morgan Lewis

31

リスクと注目度の高い訴訟への対応

- 法務チームの設置(通常、社内法務部の職員と社外顧問弁護士から構成)
- 重要な証人、意思決定者、文書管理者の特定
- 文書保存通知の発行
- 適切なプロトコルの実施によるITとデータ・セキュリティの確認
- 対外関係専門家(PR会社等)の活用について検討
- 必要に応じて企業側を代弁する広報担当者を選定

Morgan Lewis

32

Responding to High-Stakes, High-Visibility Employment Litigation

- Notify insurer (if company maintains relevant insurance policy)
- Conduct thorough investigation of allegations
- Proceed with caution before making policy changes or taking remedial actions at this juncture
 - Any modifications to company policy or remedial actions will be used against the company in litigation

Morgan Lewis

33

リスクと注目度の高い訴訟への対応

- 保険会社への連絡(適用可能な保険に加入している場合)
- 指摘された批判内容について徹底的な調査を行う
- 会社の方針・規則等の変更または対応策を実施するにあたって、慎重を期す
 - 会社の方針・規則等の変更や対応策の実施は、訴訟では企業にとって不利に使われる

Morgan Lewis

34

Takeaways

- Prepare a “break the glass” crisis management plan
- Understand and protect US attorney-client privilege protections
- Think before you write (in Japanese or English)—your emails could be exhibits in litigation
- Consider mandatory arbitration agreements and class action waivers
- Understand that globalization of Japanese initiatives must be carefully implemented in light of US laws

Morgan Lewis

35

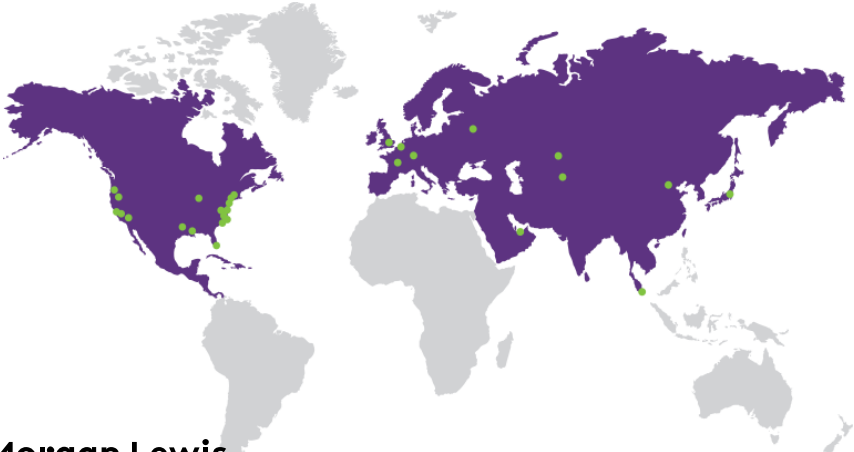
重要なポイント

- 「緊急時 (break the glass)」の危機管理対策を設定する
- 米国の弁護士・依頼者間の秘匿特権を理解し、保護する
- 日本語、英語を問わず、文書を書く前によく考える
 - 訴訟では電子メール等も証拠書類となり得る
- 仲裁合意書および集団訴訟への参加権の放棄を義務付けることを検討する
- 日本発のグローバル化は米国法を十分に考慮して、慎重に進める必要があることを認識する

Morgan Lewis

36

| | | | | | |
|-------------|---------------|--------------------|----------------------|---------------|----------------|
| ASIA | EUROPE | MIDDLE EAST | NORTH AMERICA | | |
| Almaty | Brussels | Dubai | Boston | Miami | San Francisco |
| Astana | Frankfurt | | Chicago | New York | Santa Monica |
| Beijing | London | | Dallas | Orange County | Silicon Valley |
| Singapore | Moscow | | Hartford | Philadelphia | Washington, DC |
| Tokyo | Paris | | Houston | Pittsburgh | Wilmington |
| | | | Los Angeles | Princeton | |



Morgan Lewis

THANK YOU

This material is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It does not constitute, and should not be construed as, legal advice on any specific matter, nor does it create an attorney-client relationship. You should not act or refrain from acting on the basis of this information. This material may be considered Attorney Advertising in some states. Any prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change.

© 2015 Morgan, Lewis & Bockius LLP. All Rights Reserved.

Morgan Lewis

38

Tab 2

賃金および労働時間に関連する問題を防止する方法: トップ10

1. 実際に「エグゼンプト」である者のみをエグゼンプトに分類する。(そして、適切な賃金を支給する)
2. 「研修社員」や「インターン」に対して適切な賃金を支給するよう注意を払う。
3. ノンエグゼンプトの従業員については賃金支給の対象となる作業(通勤時間外の移動時間、電子メールのチェック、ロギングイン(PCへのアクセス操作)、着替え等を含む職場外での作業)のすべてを記録し、それらの作業のすべてに対して賃金を支給する。
4. 残業手当を正確に計算し、遅延なく支給する。(通常の時給、定額給のノンエグゼンプト等)
5. 端数処理や自動控除の慣行に注意を払う。
6. 掲示を義務付けられている掲示板やポスター、資料等について、掲示を義務付けられているものはそのすべてを掲示する。(最低賃金/食事・休憩の規則等)
7. 州法に基づくすべての必要要件を遵守する。(通常より高水準の最低賃金および給与ベースの要件、通常賃金、最終賃金および有給休暇の支払のタイミング、給与支払小切手および給与支給明細書の内容、reporting time pay時給、split shift pay 分割シフト給、食事・休憩・回復(recovery)のための休み等に関する報告)
8. 賃金・労働時間に関する法律と問題について、管理職、給与管理、HRの従業員に対する研修を実施する。
9. 定期的な監査を実施し、問題点の有無を確認したうえ、問題点については是正処置を取る。
10. 従業員と契約社員/コンサルタントを適切に分類する。

Morgan Lewis

Top 10 Ways to Avoid Wage and Hour Trouble

1. Only classify those who are “exempt” as exempt (and pay them properly).
2. Record and pay nonexempt employees for ALL compensable work (noncommute travel time, offsite work such as checking emails, logging in, changing clothes, etc.).
3. Calculate and pay overtime timely and correctly (regular rate, salaried nonexempts, etc.).
4. Be careful about rounding and auto-deduct practices.
5. Post all required bulletins, posters, and materials (minimum wage, meal and rest policies, etc.).
6. Comply with all state law requirements (higher minimum wage rates and salary basis requirements; timing of regular and final wage and vacation benefit payments; content of paychecks and pay statements; reporting time pay, split shift pay, meal and rest and “recovery” breaks, etc.).
7. Train managerial, payroll, and HR employees as to wage and hour laws and issues.
8. Conduct periodic audits to learn of and correct problem areas.
9. Classify correctly employees vs. independent contractors/consultants.
10. Be careful to properly pay “trainees” and “interns.”

Tab 3

Morgan Lewis

Whistleblower Compliance Checklist

Corporate Culture

- Do you have written standards, policies, and procedures?
- Is your written code of ethics clear, comprehensive, and readily available for review?
- Have you reviewed your compliance policies to stress the importance of compliance with securities laws? Have you emphasized that employees are required to aid in maintaining compliance both by complying with the standards themselves and by reporting those who run afoul of laws?
- Have you created a culture of compliance through executive communication and training for all employees?
- Does your company conduct ongoing risk assessments?
- Have you evaluated the “tone from the top” to emphasize the importance of compliance, noting that everyone in the company shares in this responsibility and should take pride in the company’s successes in this area?
- Do you require employees to certify at least annually that they have reported to management all information they may have concerning potential violations of internal standards, policies, or the law?
- Do you enforce the standards and policies consistently through appropriate disciplinary and enforcement mechanisms?
- Do you actively make efforts to monitor compliance through audits and/or other self-evaluation methods?
- Are compliance and risk management strategic priorities of the CEO?
- Have you properly educated both the Board of Directors and senior management on the potential ramifications of the Dodd-Frank Act?
- Do your executive management and organizational leadership understand that they have specific compliance responsibilities?
- Have you established a connection among your business code of ethics, safety standards, and performance measurements?
- Do you acknowledge and reward those employees who hold themselves to the highest ethical standards?
- Do all managers have “open-door policies” for reporting issues?
- Do you clearly state that retaliation will not be tolerated against employees who report questionable behavior/activities?
- Do you train managers on behaviors that can constitute retaliation, including their responsibility to ensure that employees are not engaging in behavior that could constitute retaliation?
- Do you prohibit retaliation?

Compliance Department

- Do you have a compliance department/compliance officer?
- Do you regularly review and update internal compliance programs and audit procedures to ensure they meet current standards?
- Have you made sure your policies and procedures include prohibiting retaliation?
- Do you utilize monitoring, testing, and audit systems to assess and ensure compliance with standards and policies?
- Does your compliance department have the authority and the backing of the Audit Committee of the Board of Directors?
- Does your Chief Compliance Officer have a direct reporting line to the Audit Committee of the Board of Directors?

Document Retention Policies

- Have you implemented a comprehensive, regularly audited policy?
- Does your document retention policy include procedures for uniform and timely destruction of documents—both electronic and paper documents?
- Is your document retention policy monitored for compliance and applied consistently and companywide?
- Does your policy identify established trigger points for when documents must be retained in “anticipation of litigation” and do you initiate litigation-hold procedures when such trigger points have been reached?
- Have you created an internal incentive structure for successfully investigated complaints?

Internal Reporting Mechanisms

- Have you created user-friendly and easy-to-understand policies and procedures to encourage employees to report internally?
- Have you included a hotline to a neutral party for anonymous, confidential reports of suspected violations?
- Do you have an employee hotline and an open-door policy with direct access to Legal and Compliance personnel?
- Is your hotline well publicized? Are anonymity and confidentiality maintained and well publicized?
- Are you evaluating and implementing new reporting mechanisms such as kiosks, text messaging, and other mobile entry options to increase the convenience associated with internal reporting and to help break down barriers?
- Do your response procedures include mechanisms for logging, evaluating, investigating, and signing off on reports, and, importantly, advising complainants about the disposition of complaints?
- Do your procedures include protocols regarding who should be notified of complaints and procedures for addressing high-priority, time-sensitive complaints?
- Do you acknowledge complaints promptly?
- Do you thoroughly investigate all substantiated issues without delay?
- Are you uniform in your application of sanctions, regardless of the wrongdoer's position or status?
- Do you consider retaining outside counsel for an independent investigation on behalf of the company?
- Do you keep the complaining employee in the loop, when appropriate?
- Have you established direct lines of communication between whistleblowers and Human Resources to allow the whistleblowers to raise any situations in which they perceive they are being treated inappropriately and/or retaliated against?
- Do you document results, even if it is determined that a complaint is unsubstantiated, to create a detailed, objective report explaining how and why the conclusion was reached?
- Do you conduct background checks on all potential employees to ensure that they are not litigation risks or previous relators?
- In employment interviews, do you discuss the company's positive compliance culture?
- Do you assess each candidate's attitude toward corporate compliance in the initial interview?

Employee Education

- Do you provide education to ensure that employees understand and have confidence in the fairness and effectiveness of internal compliance procedures for reporting allegations of misconduct?
- Do you regularly educate employees about when, where, how, and to whom internal reporting can take place, and how the reports will be handled?
- Do you provide employees with understandable and accurate information regarding whistleblower laws?
- Do you regularly disseminate training materials and other information regarding company policies and the compliance program and require employee acknowledgement of these materials?
- As a matter of company policy and as required by the whistleblower statute, do you ensure that employees are aware of the benefits of internal reporting?
- Do you obtain signed acknowledgement forms from each employee and board member in which each individual states that they have received, reviewed, and understand the applicable codes and policies — and that they will adhere to them?
- Do you repeat this procedure annually?
- Do you disseminate information regularly to reinforce the culture of compliance (e.g., via annual presentations, weekly newsletters, email alerts)?
- Do you inform and ensure that employees are aware that the company will preserve and protect the anonymity of whistleblowers?
- To prevent retaliation or the perception of retaliation, are directors, executives, managers, Human Resources, and compliance personnel educated as to the conduct that may constitute retaliation under Dodd-Frank and SOX?

Termination

- Have you changed the way terminations and layoffs are conducted?
- Have you evaluated your release agreements, exit interview forms, and arbitration agreements?
- As part of the exit interview process, do you ask employees to share any concerns they may have concerning any conduct or violations of policies?

Tab 4

Reproduced with permission from Daily Labor Report, 155 DLR I-1, 08/10/2012. Copyright © 2012 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

NONCOMPETITION AGREEMENTS

Employee turnover is a fact of life, but employers can take a number of measures to minimize the risk that confidential and proprietary information will leave the building with a departing employee, Morgan, Lewis & Bockius attorneys David McManus, Prashanth Jayachandran, and Jason Burns say in this BNA Insights article. They focus on the measures an employer can take before and after learning of an employee's resignation that will help safeguard its prized intellectual assets.

The three attorneys recommend best practices employers can adopt—including executing post-employment agreements, maintaining a strict chain of custody of the employee's electronic devices, and retaining a forensic specialist if necessary—that will help put the employer in the best position possible to take action if an employee's misconduct threatens the employer's competitive advantage.

Are Your Company's Most Valuable Assets and Competitive Advantage at Risk?

BY DAVID A. McMANUS, PRASHANTH
JAYACHANDRAN, AND JASON BURNS

It is a scenario not unfamiliar to employers everywhere that rely upon superior technology and customer intelligence to survive in an increasingly competitive marketplace: without warning, a top salesperson or executive announces his resignation—effective immediately. Invariably, the departing employee is someone in whom the employer has invested significant time and resources, and who has knowledge of—and

continues to have access to—the company's most highly sensitive confidential and proprietary information. To make matters worse, the employer comes to learn that the employee intends to join a direct competitor. Under these circumstances, the employer has good reason to suspect that the employee may use its confidential information to gain a competitive advantage while working for a direct competitor.

This article focuses on the measures that an employer can take before and after learning of the employee's resignation that will help safeguard its prized intellectual assets.

First Step: Plan Ahead

The most important steps that an employer can take to limit its potential exposure in situations like the one described will occur well before the employer learns of the employee's departure. In fact, a prudent employer should have in place protective measures from the moment the employee is hired.

First, any employee who may have access to confidential and proprietary information should execute an agreement obligating the employee to safeguard and

David McManus (dmcmanus@morganlewis.com), Prashanth Jayachandran (pjayachandran@morganlewis.com), and Jason Burns (jburns@morganlewis.com) are attorneys in the Labor and Employment Practice at Morgan, Lewis & Bockius. McManus is a partner in the firm's New York office, Jayachandran is of counsel in the Princeton office, and Burns is an associate in the New York office.

protect such information and to return to the employer any and all confidential materials at any time upon the request of the employer and, certainly, at the time of the employee's separation from the company. An effective agreement will broadly delineate categories of confidential/proprietary information, documents, and other materials that the employee must protect, and prohibit the employee from disclosing or otherwise revealing to third parties confidential information without proper authorization.¹

Second, in a world in which telecommuting is the norm rather than the exception, employees who are permitted to use their own personal electronic devices to access the employer's computing and other internal IT systems should execute a separate agreement concerning the use of the employee's personal electronic devices for any work-related tasks. At minimum, the agreement should (i) require the employee to register any personal devices that the employee wishes to use for company business; (ii) authorize the employer to periodically inspect, both remotely and "in person," any registered devices; and (iii) permit the employer to inspect any registered devices and to delete any company information, and/or documents from the devices upon termination of employment.²

Third, the employer should strongly consider requiring employees to execute a noncompete agreement (assuming the employees work in a jurisdiction that permits such agreements), if they are employed in management, sales, research and design, or other positions that present the greatest threat when disclosing or using confidential information with a competitor. The agreement should be drafted by counsel familiar with the enforceability of restrictive covenants under the applicable state law.

Although requirements will vary depending on the jurisdiction, a court is most likely to uphold a carefully tailored covenant that accounts for (i) the employee's specific position, (ii) the scope and nature of the employer's business, and (iii) the potential threat posed by an employee's departure for a competitor. For this reason, employers should regularly review restrictive covenants to ensure that they reflect for each employee the appropriate circumstances of employment.

Any confidentiality or restrictive covenant agreement should specifically acknowledge that a breach of its

¹ The scope of the information covered under any confidentiality agreement must not be so broad as to potentially interfere with an employee's rights under applicable laws, including Section 7 of the National Labor Relations Act. Section 7 prohibits employers from interfering with employees engaged in certain "concerted activity" with respect to the terms and conditions of their employment, which in some circumstances may include employee comments about workplace conditions on social media sites such as Facebook. See, e.g., *Hispanics United of Buffalo, Inc.*, NLRB ALJ, No. 03-CA-027872 (173 DLR AA-1, 9/7/11) (Sept. 2, 2011).

² Employers should ensure that any agreement concerning the employee's personal computing devices complies with applicable laws restricting employers' access to information about employees' use of social networking sites. For example, two states, Illinois and Maryland, have recently passed laws that prohibit employers from, among other things, requesting from employees access information related to the employees' social media accounts. A handful of other states are considering similar laws, including Delaware, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, South Carolina, and Washington.

terms will entitle the company to injunctive relief, a factor that will weigh in the employer's favor should the employer ever seek to enjoin the employee from violating the agreement. See, e.g., *CentiMark Corp. v. Lavine*, No. 11-0757, 2011 BL 196078 (W.D. Pa. July 28, 2011) (granting preliminary injunction in part because employee acknowledged that breach of post-employment obligations would entitle employer to injunctive relief); *Ayco Co., L.P. v. Feldman*, 10-CV-1213, 2010 BL 250395 (N.D.N.Y. Oct. 22, 2010) (evidence of employer's irreparable harm may be found in employee's breach of a post-employment competition provision that provides that the breach will (i) leave the employer without an adequate remedy at law and (ii) entitle the employer to injunctive relief).

Second Step: Take Swift and Immediate Action When an Employee Departs to a Competitor

Responding promptly to news of an employee's departure will mitigate any potential losses or damage that might result from any employee misconduct or foul play. Swift action will also allow an employer to begin building its case in the event legal action becomes necessary to protect the company's confidential and proprietary information.

Any time an employee separates from a company, either voluntarily or involuntarily, the employer should remind the employee, in writing, of his or her obligations under any confidentiality, noncompete, or other applicable agreements. Likewise, the employer should seek from the employee written assurance that he or she has complied with any restrictive covenants.

If the employee has disclosed that he or she is joining a competitor, the employer should consider notifying that competitor, potentially through counsel, of the employee's post-employment contractual obligations. This way, the new employer will be put on notice about the employee's post-employment obligations and may take measures to ensure that the employee complies with these obligations. If the competitor fails to satisfactorily address this matter, taking this step may bolster an employer's ability to obtain injunctive relief, as the employer can demonstrate to a court that the employer's own efforts to resolve the matter were unsuccessful and that judicial intervention is necessary.

It is important that any communications with the employee's new or potential employers be confined to the facts surrounding the employee's departure (e.g., the scope of the employee's obligations under a confidentiality agreement or the existence of any pending legal action related to the enforcement of that agreement). By keeping the discussion to the "facts," the employer can limit its exposure to potential claims by the employee for defamation or interference with business relations.

If it is not the employer's regular practice to review the email and computing devices of departing employees to ensure that they have not misappropriated any confidential information, the employer should immediately perform a forensic analysis of the computing devices, including any devices subject to a personal computing agreement (e.g., PDAs, smartphones, etc.), of any employee joining a competitor and/or whom the employer suspects may have retained, transferred, or otherwise disclosed confidential and proprietary information.

Similarly, the employer should review any of its internal data systems to determine whether the employee

has engaged in any unauthorized access or other activity that raises any red flags (e.g., sending company documents to a personal email address or using a USB device to download documents within days of announcing his or her resignation). In any event, the employer should meticulously document the chain of custody of the computing devices for any departing employee in order to bolster the employer's ability to prove that the departing employee was directly responsible for the misconduct and to rebut any potential claims of spoliation.

In addition to potentially uncovering a complete record of any employee misdeeds, a third-party analyst may be a valuable resource for evidence against the employee. See, e.g., *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357 (S.D. Fla. 2009); *Pharmerica, Inc. v. Arledge*, 8:07-cv-00486-RAL, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007) (relying on evidence gathered from third-party forensic analyst to find that employee had systematically copied and deleted employer's confidential and trade secret information).

Continental Group is instructive on this point. There, the plaintiff's forensic expert testified at length at the preliminary injunction hearing that the employee downloaded voluminous files to her personal laptop and personal portable data storage devices in the days leading up to her resignation. The court specifically acknowledged that it found this testimony credible and "relied on it extensively" in compelling the employee to, among other things, return all confidential documents and data to the employer. Thus, promptly retaining a reputable outside expert can be critical to an employer's litigation preparedness and strategy.

Third Step: Initiate Litigation if Necessary

If the employee refuses to fully comply with the employer's demands to return all confidential information or abide by his/her restrictive covenant agreements, the employer may have no choice but to initiate legal action against the former employee and, perhaps, the employee's new employer. In fact, failure to do so may undermine an employer's ability—in subsequent similar claims involving other employees—to demonstrate that the information that it is seeking to protect is "confidential" and that the employer will suffer irreparable harm in the event of its disclosure, as described below.

Because of the urgent need to protect confidential information, a temporary restraining order, to be followed by preliminary injunctive relief, will likely be the most expedient method for protecting the employer's business interests.

Although the standard for issuing a preliminary injunction differs depending on the jurisdiction, employers seeking to enjoin a former employee from disclosing confidential information typically must satisfy the test set forth by the U.S. Supreme Court in *Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7 (2008): (1) that the employer will suffer irreparable harm in the absence of preliminary relief, (2) that the employer is likely to succeed on the merits, (3) that the balance of equities tips in the employer's favor, and (4) that an injunction is in the public interest. Of course, whether an employer will be entitled to injunctive relief will depend on the individual circumstances surrounding the employee's departure.

In any action for a preliminary injunction, establishing a likelihood of irreparable harm is the single most important prerequisite for obtaining relief from the court. *Faively Transportation Malmö AB v. Wabtec Corp.*, 559 F.3d 110 (2d Cir. 2009). An employer may establish irreparable harm by showing that violation of the employee's post-employment restrictive covenants will result in the loss of client relationships and customer good will that has been built up over time, or in the loss of confidential customer information. See, e.g., *North Atlantic Instruments, Inc. v. Haber*, 188 F.3d 38, 15 IER Cases 731 (2d Circuit 1999); *CentiMark Corp. v. Lavine*, No. 11-0757, 2011 BL 196078 (W.D. Pa. July 28, 2011); *Mintel Int'l Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2008 BL 149547, 27 IER Cases 1876 (N.D. Ill. July 16, 2008); *Johnson Controls, Inc. v. A.P.T. Critical Systems, Inc.*, 323 F. Supp. 2d 525 (S.D.N.Y. 2004). Even where an employee insists that he or she has not misappropriated any confidential customer information, a court is unlikely to credit such testimony where other evidence demonstrates that the employee contacted an employer's customers shortly after his or her departure. See *Ayco Co., LP. v. Frisch*, 795 F. Supp. 2d 193 (N.D.N.Y. 2011).

Courts have also found irreparable harm where a former employer has demonstrated that the disclosure of proprietary information will allow a competitor to "cut corners" in the research and development process, thus accelerating the competitor's introduction of a product into the marketplace. See *Universal Engraving, Inc. v. Duarte*, 519 F. Supp. 2d 1140 (D. Kan. 2007) (finding irreparable harm where employee joined competitor to assist in research and design of products similar to those manufactured by former employer). Similarly, an employer can show that it may suffer from unfair competition if an employee familiar with the employer's confidential business and marketing strategies joins a direct competitor. *Nike Inc. v. McCarthy*, 379 F.3d 576, 21 IER Cases 1089 (9th Cir. 2004) (157 DLR AA-1, 8/16/04).

Courts have also found irreparable harm where a former employer has demonstrated that the disclosure of proprietary information will allow a competitor to "cut corners" in the research and development process, thus accelerating the competitor's introduction of a product into the marketplace.

In *Nike*, the Ninth Circuit affirmed an injunction enforcing a noncompete agreement against a former Nike executive who resigned from the company to join Reebok. The court found that because the executive had intimate knowledge of Nike's "product allocation, product development and sales strategies," he could develop business and marketing strategies for Reebok that "could divert a substantial part of Nike's footwear sales to Reebok based on his knowledge of information con-

fidential to Nike,” even “without explicitly disclosing this information to any of Reebok’s employees.”

When an employee has misappropriated confidential information stored on an employer’s computing systems, including email systems, an employer should consider asserting claims under the federal Computer Fraud and Abuse Act (CFAA) or equivalent state laws. Under the CFAA, an employer can bring a claim against a former employee whose unauthorized access of a protected computer results in losses or damages of at least \$5,000. 18 U.S.C. § 1030 et seq. In pursuing a CFAA claim, an employer will benefit significantly by demonstrating through forensic analysis the extent of the employee’s misconduct. See *Universal Engraving, Inc. v. Duarte*, 519 F. Supp. 2d 1140 (D. Kan. 2007) (finding that results of employer’s forensic analysis discredited testimony of former employee who denied accessing his work computer on the dates in question); *Pharmerica, Inc. v. Arledge*, 8:07-cv-00486-RAL, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007) (relying on employer’s forensic review of former employee’s computer to find likely violation of CFAA).

A benefit of asserting CFAA claims is that an employer may be able to recover certain costs and fees related to the investigation of the employee’s misconduct that are not otherwise recoverable under common law absent a contractual agreement with the employee providing for the recovery of such fees. See, e.g., *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001) (holding that a plaintiff may recover under the CFAA costs incurred by hiring a forensic computer consultant to assess and diagnose the extent of a party’s unauthorized computer access).

Often, the situation will arise where, prior to separating from the employer, an employee allegedly exceeds his or her computing authority by obtaining for an improper purpose that information which the employee is otherwise permitted to access. Although courts have reached different results in this area, several courts have found that an employer may state a claim under the CFAA when the employee downloads proprietary information for the employee’s own benefit or for the benefit of a competitor. See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (finding that employer was likely to prove unauthorized access under the CFAA where former employee provided proprietary information to new employer in violation of his confidentiality agreement); *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357 (S.D. Fla. Apr. 2009) (even though employee had access to employer’s password-protected files, she exceeded her authority by downloading certain files after she began negotiating to join competitor).

In some circumstances, an employee may exceed authorized access under the CFAA by sending to a personal email address, in the days leading up to resignation, an employer’s confidential information regarding its client accounts and marketing strategies. See *Mintel International Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2008 BL 149547, 27 IER Cases 1876 (N.D. Ill. July 16, 2008). Indeed, where the scope of an employee’s authorized access is at issue, an employer can bolster its case by showing that the employee did not have a legitimate business reason for accessing or downloading the files in question or that the employee copied or downloaded the information immediately prior to his or her

resignation. See *Continental Group, Inc. v. KW Property Management, LLC*, 622 F. Supp. 2d 1357 (S.D. Fla. Apr. 2009); *Mintel Int’l Group, Ltd. v. Neergheen*, No. 08-CV-3939, 2008 BL 149547, 27 IER Cases 1876 (N.D. Ill. July 16, 2008).

An employer may also seek injunctive relief under the CFAA if an employee, in an attempt to “cover his tracks,” permanently deletes without authorization the employer’s files and emails. *Pharmerica, Inc. v. Arledge*, 8:07-cv-00486-RAL, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007).

Typically, where an employer has satisfied the elements for issuing a preliminary injunction, the court will grant an employer’s request that the employee refrain from disclosing, transferring, or otherwise using the confidential information at issue. See, e.g., *Redwood Software, Inc. v. Urbanik*, No. 12-cv-0495, 2012 BL 80632 (N.D.N.Y. Mar. 30, 2012) (Decision and Order); *Universal Engraving, Inc. v. Duarte*, 519 F. Supp. 2d 1140 (D. Kan. 2007); *Hudson Global Resources Holdings, Inc. v. Hill*, No. 07-CV-00132, 2007 BL 190879 (E.D. Pa. May 25, 2007). That said, courts have been reluctant to order employees to turn over personal computing devices for inspection and forensic analysis, particularly where the court has already enjoined the employee from using or disclosing confidential information that might otherwise remain on the employee’s personal devices. See *PLC Trenching Co., LLC v. Newton*, No. 11-CV-05015, 2011 BL 124067 (N.D.N.Y. May 10, 2011). In *PLC Trenching*, the court found that the forensic investigation requested by the employer was unnecessary given (1) the ethical obligation of the employee’s attorney to ensure that his client complied with that part of the court’s order enjoining the employee from transferring or otherwise disclosing the employer’s confidential information and that (2) if necessary, the employee could seek the information at a later date, for example during the course of discovery.

Accordingly, execution of a “personal computing agreement,” as described above, may provide an alternative basis for the court to order a forensic review of non-employer issued computing devices. And a court might be more receptive to ordering an employee to turn over his or her personal devices if the proposed review is to be conducted by an independent, third-party forensic analyst and the employee is given an opportunity to identify and seek protection of objectionable information (such as attorney privileged information) on the devices. See *Ryan, LLC v. Evans*, 8:12-CV-289-T-30TBM (M.D. Fla. Mar. 20, 2012).

Not surprisingly, courts are most likely to compel an employee to produce for review forensic copies of personal computing devices in those cases where the employer has made a strong showing that an employee has misappropriated confidential information and that such misconduct is likely to result in irreparable harm. This was the case in *Pharmerica, Inc. v. Arledge*, No. 08-CV-3939, 2007 BL 234119 (M.D. Fla. Mar. 21, 2007). There, the court ordered a former employee to turn over to the court all of the employee’s computers, USB storage devices, hard drives, PDAs and other electronic devices. Significantly, the employer produced to the court evidence from a forensic analyst demonstrating that the employee had downloaded to a USB storage device, and then permanently deleted, hundreds of confidential documents in the weeks leading up to the employee’s defection to a competitor.

Conclusion

Employers can adopt several best practices to protect their most important customer, technical, and strategic information:

- Insist that employees with access to confidential and proprietary information execute post-employment agreements that will protect that information from disclosure to competitors and other third parties.
- Respond promptly to contain potential damages or losses that might be caused by departing employees, including notifying employees and their new employers of the employee's obligations under any post-employment agreements.
- Where there is evidence that an employee has downloaded and/or obtained confidential/proprietary information, maintain a strict chain of custody for the employee's devices and consider promptly retaining a

reputable and experienced forensic analyst to document and assess the extent of the employee's unauthorized access.

- Should judicial intervention become necessary, demonstrate the specific harm that the company will suffer absent the requested relief by highlighting the scope of the employee's unauthorized access and any peculiar circumstances surrounding the employee's departure (e.g. downloading confidential documents immediately prior to joining a competitor).

Employee turnover is a fact of life for all companies. But, as discussed above, employers can take a number of measures to minimize the risk that confidential and proprietary information will "leave the building" with a departing employee and to put the employer in the best position possible to take action when an employee's misconduct threatens the employer's competitive advantage.