Hot Topics and Trends in Insurance Coverage

11th Annual Hospitality Law Conference in Houston, Texas

February 11-13, 2013

John E. Heintz
Kenneth Berline Trotter
Dickstein Shapiro LLP
1825 Eye Street NW
Washington, DC 20006-5403

DICKSTEIN SHAPIRO LLP

John E. Heintz	**Kenneth Berline Trotter**
1825 Eye Street NW Washington, DC 20006-5403 Tel (202) 420-5373 HeintzJ@dicksteinshapiro.com www.DicksteinShapiro.com	1825 Eye Street NW Washington, DC 20006-5403 Tel (202) 420-2912 TrotterK@dicksteinshapiro.com www.DicksteinShapiro.com

John E. Heintz is a partner in Dickstein Shapiro's Insurance Coverage Practice. A veteran in the fields of corporate insurance coverage and complex litigation with more than 30 years of experience, Mr. Heintz has won numerous landmark appellate cases in state and federal courts, and he has recovered billions of dollars in coverage for his clients. He has represented clients in securing coverage for property and business interruption losses arising out of the 9/11 attacks, hurricanes, and other catastrophic events. The 2012 *Chambers USA* ranks Mr. Heintz as one of the top 12 leading insurance coverage attorneys in the country. *Chambers* states that "he is known to peers as 'one of the best lawyers in this field,'" noting that "he is described as 'an outstanding performer with an outstanding reputation.'" The 2012 edition of *Legal 500* recognized Mr. Heintz as a "leading lawyer" in the Insurance: Advice to Policyholders category and "among the very best." Mr. Heintz has also been recognized by *Expert Guides*, *Super Lawyers*, *Who's Who Legal*, *Lawdragon*, *Law 360*, and *The Best Lawyers in America*. Mr. Heintz and his co-authors were selected as Burton Award winners for the 2010 "Distinguished Law Firm Category" for their article "Insurance Coverage for Climate Change Suits: The Battle Has Begun," which was published in *The Environmental Claims Journal* in March 2009.

Kenneth Berline Trotter is a Washington, DC-based attorney in Dickstein Shapiro's Insurance Coverage Practice and devotes a significant portion of his practice to the representation of policyholders in complex insurance disputes with their insurance companies. On insurance claims matters, he has assisted policyholders in pursuing property and business interruption claims including claims resulting from hurricanes, floods, the events of 9/11, and other catastrophes. His client representations include litigation in both state and federal courts and various forms of alternative dispute resolution. He has written articles for numerous publications involving the hospitality industry including *Lodging*, *Southern Hospitality Professional*, *Hospitality Upgrade*, *Seafood Business*, and *Hospitality Lawyer In-House Counsel Newsletter*. Mr. Trotter currently is co-leader of the firm's Property and Business Interruption Insurance Coverage Initiative.

Table of Contents

SCOPE OF ARTICLE

The hospitality industry has experienced unprecedented losses and liabilities in the new millennium as a result of such events as: hurricanes, earthquakes, tsunamis, cyber attacks and data breaches, 9/11, terrorism in Mumbai and the Arab Spring, and employee class actions. These events have seriously threatened the very economic survival of many hospitality businesses. And many hospitality businesses have suffered economic losses as a result of an event even though it took place hundreds or thousands of miles away.

These events highlight the importance of risk management – in the broadest possible sense of that term – and of insurance as a central component in any risk management strategy. Many businesses that were damaged by these events have learned the hard way that their current insurance programs did not adequately cover these risks or did not provide the coverage that they thought or assumed they had purchased. Businesses that were not damaged by these events should use these events to examine their own insurance programs and evaluate whether they would have been protected. For example, would the business have insurance coverage for lost income caused by an evacuation order issued in advance of a hurricane? Would the business have insurance coverage for loss and liabilities caused by data thieves hacking into the company's computer systems containing confidential consumer data that is protected by privacy laws? Would the business have coverage for economic loss at business operations in another country caused by the action of a foreign government that restrains the company's business operations? This paper presents some practical considerations for in-house counsel, risk managers, and business managers, in conducting such a "what if" analysis.[1]

I. COVERAGE FOR SUPERSTORM SANDY

Superstorm Sandy's strike at the heart of the most densely populated area of the country caused loss of life, destruction, and dislocation on a massive scale. Its economic impact will be felt by businesses and individuals across the country for some time. Obviously, many businesses suffered direct damage to property and lost income due to the resulting interruption of their operations, but many other businesses have also lost substantial income due to evacuation orders, disruption of utility service, disruption of mass transit on which their employees rely to get to and from work, and disruption of the operations of key suppliers or customers. Loss estimates now exceed $50 billion, and are certain to go higher.

There is no doubt that recovering insurance for much of these losses will be as complicated and challenging as has been the case with 9/11 and Hurricane Katrina. Specifically, property insurance, including business interruption and contingent business interruption coverages, protects against more than just physical damage to and loss of property. Such insurance also often protects against financial losses arising from an inability to conduct business (either at all or at the same levels as before) because of property damage, orders of civil authorities, or the inability to access business premises; the extra expenses incurred in dealing with the effects of a disaster, including money spent to minimize any damage and losses; and the costs incurred in establishing the extent of the losses. Moreover, contingent business interruption coverage often contained in first-party property policies may provide coverage when a business faces loss due to its suppliers' inability to provide needed goods and services, or its

[1] The authors would like to thank Scott N. Godes and Kristin Davis, a counsel and an associate, respectively, at Dickstein Shapiro, for assisting in preparing portions of this paper.

customers' inability to patronize a business. Other types of insurance that also may respond include policies for trade disruption, event cancellation, and directors and officers. Specific policy language and particular circumstances may impact the availability and scope of coverage significantly. Indeed, how the cause of loss is characterized may affect the applicability and amount of deductibles, sub-limits, and coverage extensions.

A business that faces losses from any major storm event should immediately consider how its insurance will respond, assess its insurance policies, and develop a plan to determine and document losses that were or will be sustained because of the disaster. Experience tells us that even sophisticated businesses unknowingly commit errors in assessing and documenting their losses or interpreting their insurance policies that later limit or even bar potential insurance recovery, and that insurers frequently use initial characterizations or "labels" as a basis to restrict or eliminate coverage.[2]

II. INSURANCE COVERAGE FOR CYBER RISKS

Hospitality firms face increasing exposure to risks arising from their collection of data and electronically stored information. Although the ability to compile and store such information cheaply in a way that allows easy access and manipulation has helped companies improve service to their customers and has given companies access to a considerable amount of information about those customers, this data also makes the company vulnerable to losses, whether by corruption of data or direct attack from malicious individuals or software. For example, electronic collections of customer data on computer networks – credit card numbers in particular – are attractive targets to hackers. Indeed, a report by Willis Group Holdings, a British insurance firm, states that the largest share of cyber attacks – 38% – were aimed at hotels, resorts, and tour companies. According to the report, insurance claims for data theft worldwide jumped 56% in 2011, with an increasing proportion of those attacks targeting the hospitality industry. Because businesses in the hospitality industry obtain and maintain confidential data from consumers – countless credit card records in particular – they will continue to be attractive targets for hackers and data thieves.

Managing such risk is critical to successfully navigating in the business world in the new millennium. The financial security and stability of a company depend upon more than just the protection of the company's proprietary data and information. The company must also be protected from liability to third parties or the government for data breaches that are difficult to predict, and over which the company often has little control. Because hackers and programmers of malicious software wage a cutting-edge war against those that make databases and networks more secure and reliable, often the best protection a company can get is protection against the consequences of a data breach. Companies can find protection in both traditional forms of insurance and new forms of specialty insurance being introduced to the market for these new potential risks and liabilities.

[2] For a comprehensive examination of these issues, please see the forthcoming white paper, "Superstorm Sandy: An Overview of Insurance Coverage for Losses Associated with the Storm," authored by John E. Heintz and co-authored by Kirk A. Pasich and Jared Zola, to be published by LexisNexis and available on-line.

A. Cyber Risks – Cyber Attacks And Data Breaches

Two of the most well-known cyber risks are cyber attacks and data breaches. One form of cyber attack is a *denial of service* incident. Denial of service attacks may be designed to bring a website or service down, preventing customers from accessing the site or the company's products or services. One research and development center has explained that denial of service attacks come in a variety of forms. The three basic types of denial of service attacks are: consumption of scarce, limited, or non-renewable resources; destruction or alteration of configuration information; and physical destruction or alteration of network components.[3] Some cyber attacks are comparable to "tak[ing] an ax to a piece of hardware" and may be called "permanent denial-of-service (PDOS) attack[s]."[4] If a system suffers such an attack, which also has been called "pure hardware sabotage," it "requires replacement or reinstallation of hardware."[5]

Another cyber risk, perhaps more widely discussed in the news, is a *data breach*. The term data breach is used broadly, usually to describe incidents in which hackers, rogue current or former employees, or others steal or otherwise gain access to personally identifiable information or personal health information. For example, in *Anderson v. Hannaford Brothers Co.*, the court described a data breach against "a national grocery chain whose electronic payment processing system was breached by hackers . . . [with] hackers [having] stole[n] up to 4.2 million credit and debit card numbers, expiration dates, and security codes . . . ."[6]

B. First-Party Losses And Third-Party Liabilities Arising Out Of Cyber Events

A cyber attack can result in *first-party risks* to the company. These may include, for example: physical damage to, loss of, or loss of use of data and software only, whether caused by a third party, a contractor, an employee/former employee, a state actor, or a "cyber war" or "cyber terrorism"; corrupted, lost, stolen, or ransomed data resulting from data theft, data breach, or virus; loss of use of data as a result of software failure, network interruption, or denial of service attack; and an inability to conduct business because of loss of software, data, or network access.

In addition, data breaches may result in two significant types of *third-party claims* against the company. First, consumers have filed class action lawsuits alleging, among other things, the loss of the value of their personal information, identity theft, invasion of privacy, negligence, or

---

[3] CERT, *Denial of Service Attacks*, http://www.cert.org/tech_tips/denial_of_service.html (last visited Jan. 4, 2013); CERT, *About [CERT]*, http://www.cert.org/meet_cert/ (last visited Jan. 4, 2013).

[4] *See* Kelly Jackson Higgins, *Permanent Denial-of-Service Attack Sabotages Hardware*, Security Dark Reading, http://www.darkreading.com/security/management/showArticle.jhtml?articleID=211201088 (May 19, 2008).

[5] *Id.*

[6] 659 F.3d 151, 154 (1st Cir. 2011).

contractual liability. For example, in 2011, Sony allegedly suffered various cyber attacks and data breaches, leading to multiple putative class action lawsuits against various Sony entities.[7]

Second, governmental entities such as the Federal Trade Commission ("FTC") and state attorneys general have aggressively pursued companies for alleged failures to maintain reasonable security measures to protect consumers' sensitive data. In a case involving a business in the hospitality industry, the FTC alleged that a company's failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks on multiple occasions and that the company's security failures led to millions in fraudulent charges on consumers' accounts, and the export of thousands of consumers' payment card account information to a domain registered overseas. The company is contesting the suit and the FTC's authority to bring it. Outside of the hospitality industry, in 2009, TJX Companies, Inc. agreed to pay $9.75 million to 41 attorneys general as part of a settlement that followed an investigation concerning the retailer's data security practices.[8]

Consumer and governmental actions expose a company to significant liability if the allegations prove to be true. Even if the allegations or claims are unfounded or groundless, however, a company also may spend significant sums in legal expenses to defend itself against such actions. According to a new white paper from NetDiligence, legal damages accounted for the majority of the $3.7 million average cost per data breach that occurred between 2009 and 2011.[9]

In addition, companies may face claims from business partners alleging breach of contract, negligence, or other causes of action, or demanding contractual defense and indemnity, resulting from a data breach or other cyber event. For companies with international operations, it is significant to keep in mind that cyber security is an international issue:

> Today, cybercrime has become an organized underground economy reaping vast financial rewards using sophisticated software tools that threaten users and information infrastructures in all countries.[10]

---

[7] *See, e.g.*, Complaint ¶ 101, *Johns v. Sony Corp.*, No. 3:11-cv-02063-RS (N.D. Cal. Apr. 27, 2011) ("Sony Claims"). In addition to the Sony Claims brought by third parties, Sony reportedly suffered a nine-figure loss as a result of the first hack. *See, e.g.*, Alastair Stevenson, *Sony Networks Hacked Post-PSN and PlayStation Store Restart*, Int'l Bus. Times (June 3, 2011), http://uk.ibtimes.com/articles/156879/20110603/sony-hack-lulzsec-security-psn-playstation-network-hackers-security-breach-3-4.htm.

[8] Press Release, Washington State Office of the Attorney General, Attorney General McKenna Calls TJX's Data Breach a Costly Lesson (June 23, 2009), http://www.atg.wa.gov/tjxsettlement062309.aspx.

[9] NetDiligence, *Cyber Liability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches* at 4 (Oct. 2012), http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf.

[10] Sami Al Basheer Al Morshid, Opening Remarks, Regional Cybersecurity Forum (Feb. 18, 2008), http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/opening-remarks-itu-al-basheer-feb-08-english.pdf.

Accordingly, companies with international operations face the additional challenge of managing risks, and complying with applicable governmental regulations, both within the United States and abroad.

C. Insurance Coverage For Cyber Risks

A company should analyze its entire slate of insurance policies to determine in advance of any breach what coverages might apply to cyber risks, in both the first-party and third-party contexts. Companies should consider purchasing a policy designed specifically for cyber risks, sometimes referred to as "cyber insurance." More traditional forms of insurance may also provide coverage for data breaches and cyber risks, depending on the particular coverage terms and exclusions in the individual policy. In addition to cyber insurance, coverage may be provided by the following types of policies, *inter alia*: Commercial General Liability ("CGL"); First-Party Property and Business Interruption; Directors and Officers ("D&O") or Errors and Omissions ("E&O"); Crime; Kidnap, Ransom, and Extortion; and Professional Liability.

1. Cyber Insurance

Cyber insurance may be a good solution for many companies, particularly those that rely heavily on computer networks in the business operations or maintain large databases of consumer information. Such insurance is marketed expressly for cyber-related loss. Cyber insurance comes in many forms and variations, including: Technology E&O, Information Security Insurance, Network Security Insurance, Privacy Insurance, Data Breach Insurance, Network Breach Insurance, Technology Solutions, and a wide variety of trade names that seem to incorporate the term "tech," "cyber," or some form of "digital." The Insurance Services Office, Inc., which develops and seeks regulatory approval for many insurance policy forms and language, has a standard insurance form called the "Internet Liability and Network Protection Policy," and insurance companies may base their coverages on this form, or they may provide their own company-worded policy form. Because these "cyber insurance" policies are frequently updated and changed, it is important to compare the coverages offered across companies and within a company's offerings. These forms vary, so it is critical that those involved in the procurement of such policies carefully consider and compare the basic insuring agreements, limitations, exclusions, and conditions in the policy.

A properly designed cyber insurance solution may very well preempt a difficult explanation to senior management that, after a cyber loss, the insurance company denied coverage under other lines of insurance, even if the denial was not warranted. When reviewing cyber insurance policies, it is important to consider whether there is coverage for so-called first-party risks and third-party risks. Key considerations, when purchasing cyber insurance, include:

- Does the policy respond to costs incurred because of liabilities that require the insured to take steps to remedy a breach of personally identifiable information, even if there is not a demand made by a claimant or governmental entity?

- Does the policy address coverage for liabilities to the payment card industry?

- Does the policy cover regulatory investigation and actions, such as actions brought by the FTC and state attorneys general? If so, how formal must an investigation be

before the coverage applies? How is a covered "action" defined? Are investigatory subpoenas covered?

- How broadly does the policy define "computer system" or "network" and information in the care, protection, or control of third parties, including those with written contracts and those without?

- Does the policy provide coverage for identity theft resolution services, including the costs associated with notifying individuals about the breach, credit monitoring expenses for individuals whose information was leaked, as well as credit counseling services, credit restoration services, and even identity theft resolution services? (The optimal policy will provide such coverage even when the notification is voluntary and there is no law requiring such notification.)

- Does the policy provide coverage for loss control services? (A company should consider, however, whether the coverage it purchases is contingent upon its agreeing to perform any security upgrades recommended by the loss control services company.)

- Does the policy pay for the costs of data restoration?

- Does the policy cover liabilities arising out of injuries to companies, corporations, partnerships, and other entities, as well as natural persons?

- What are the geographic limitations of the policy? Does the policy apply to a data breach involving data stored outside of the company's offices (e.g., data stored with "cloud" providers and other vendors that may host data outside of the United States)?

The core and unique elements of cyber insurance are included within the offered policy:

Coverage for First-Party Risks[11]

- **Data/Electronic Information Loss**
  - Covers the costs of recollecting or retrieving data destroyed, damaged, or corrupted due to a computer attack.
- **Business Interruption or Network Failure Expenses**
  - Covers the costs of lost net revenue and extra expense arising from a computer attack and other human-related perils. Especially valuable for computer networks with high availability needs.
- **Cyber-Extortion**
  - Covers both the costs of investigation and the extortion demand amount related to a threat to commit a computer attack, implant a virus, etc.

[11] As to first-party risks, companies should carefully analyze the trigger of coverage in the cyber policy. The trigger for such coverage should not be limited to a "physical" cause of loss or to "tangible" property and should be broad enough to include cyber attacks, data breaches, hackings, and other cyber events.

Coverage for Third-Party Risks

- **Network Security Liability**
  - Claim expenses and damages emanating from network and non-network security breaches.
- **Media Liability**
  - Claim expenses and damages emanating from personal injury torts and intellectual property infringement (except patent infringement).
  - Claim expenses and damages emanating from electronic publishing (website). Some policies will provide coverage for all ways in which a company can utter and disseminate matter.
- **Privacy Liability**
  - Claim expenses and damages emanating from violation of a privacy tort, law, or regulation.
  - Claim expenses and damages emanating from a violation of a law or regulation arising out of a security breach.[12]
- **Privacy Regulatory Proceeding and Fines**
  - Claim expenses in connection with a privacy regulatory inquiry, investigation, or proceeding.
  - Damages/fines related to a consumer redress fund.
  - Privacy regulations fines.
  - PCI liabilities.
- **Privacy Event Expense Reimbursement**
  - Expense reimbursement for third-party forensics costs.
  - Public relations costs.
  - Legal expenses.
  - Mandatory notification costs (compliance with security breach notification laws) and voluntary notification costs.[13]
  - Credit monitoring costs.
  - Call center costs.
  - Second security audits required by financial institutions (this coverage varies by market).

[12] Businesses should consider what damages are covered, and whether damages arising out of state-based consumer protection acts are covered. Although many non-cyber insurance policies may purport to exclude such damages, data breach-based class actions often seek such damages. *See, e.g.*, Complaint at 11-19 (Causes of Action), *Johns v. Sony Corp.*, No. 3:11-cv-02063-RS (N.D. Cal. Apr. 27, 2011).

[13] With respect to coverage for third-party liabilities, companies should consider whether their cyber insurance policies provide coverage for privacy breaches, even before there has been a "claim," to ensure that coverage exists for costs incurred immediately after the discovery of a data breach, including investigation and notification costs. (These costs may be referred to as "voluntary notification" costs among those in the industry, though they may not truly be voluntary.)

2. Coverage Under Traditional Insurance Policies (E.g., Property, CGL)

Coverage for cyber-related liabilities may also be available under traditional forms of coverage, such as first-party property policies and CGL policies. Insureds, however, should not assume that their insurance companies will agree that coverage is provided by more traditional forms of insurance notwithstanding positive case law. For example, Zurich, seeking to avoid defending or indemnifying Sony against the Sony Claims, filed an action against numerous Sony entities seeking declarations that there is no coverage under various CGL policies, among other requests for rulings.[14] The matter is still pending and the outcome remains uncertain, particularly when Zurich itself previously had recognized, in at least one article, that "[t]hird-party liability policies such as Commercial General Liability (CGL) policies provide coverage to a company . . . [for] data security breaches."[15]

D. Companies Should Be Cognizant Of The Potential For Claims Against The Company And Its Directors And Officers Relating To Cyber Risks And Alleged Failures To Insure Against Cyber Risks

On October 13, 2011, the Division of Corporation Finance of the Securities and Exchange Commission ("SEC") issued CF Disclosure Guidance: Topic No. 2, "Cybersecurity."[16] The Guidance recognizes the "increasing dependence on digital technologies" for registrants "to conduct their operations." The Guidance suggests that registrants consider the "adequacy of their disclosure relating to cybersecurity risks and cyber incidents" and that "appropriate disclosures may include . . . Description of relevant insurance coverage." This recent Guidance has caught the attention of companies and commentators, including the emphasis on the disclosure of insurance coverage. Commentators have suggested that, in light of the Guidance, companies should be cognizant of the potential for D&O risks for failure to manage and insure IT risk.[17] Whether such claims are seen as meritorious or not, companies in the hospitality industry should be aware of and consider the Guidance, and have an understanding of the scope of the company's "relevant insurance coverage" for cyber risks.

---

[14] *See* Complaint, *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011 (N.Y. Sup. Ct. July 20, 2011).

[15] Zurich, *Data Security: A Growing Liability Threat*, http://www.zurichna.com/internet/zna/SiteCollectionDocuments/en/media/whitepapers/DOCold2DataSecurity082609.pdf.

[16] The Guidance may be viewed at: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[17] *See* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. Marshall J. Computer & Info. L. 313, 318-19 (2011) ("In light of recent large cyber attacks, the SEC has issued new disclosure guidance requiring public companies to disclose cybersecurity risks that reasonable investors would consider important to investment decisions and how they address them, including whether they have cybersecurity or privacy insurance.").

III. POLITICAL RISK INSURANCE

As more companies are doing business in more places around the world, political risk insurance is becoming a hot new area. Political risk refers to a wide range of risks, including some of interest to many risk managers which may not come to mind when one thinks of political risks. The type of political risk that gets the most attention is loss associated with political violence, terrorist attack, or civil unrest, like the losses that resulted from the terrorist attacks in Mumbai or the Arab Spring protests in Egypt and subsequent civil wars in Libya and Syria.[18] These types of losses are hard and/or expensive to insure in areas such as the Middle East. However, the most commonly insured type of political risk involves such risks as a host government frustrating or repudiating a contract with an international company, for instance, to build a facility for which the company expects a certain rate of return, or the risk that a foreign government may expropriate or confiscate assets, like the Cuban government did in the 1960s. Political risk also includes a foreign government wrongfully calling a line of credit or guarantees or currency inconvertibility or the inability to repatriate funds. Political risk insurance is available to cover these types of risks.

Political risk insurance differs from traditional commercial general liability and first-party policies in several ways. One of the main differences is that the insurance carrier can be either a public entity or a private entity. These public or "official" providers are the Multilateral Investment Guarantee Agency ("MIGA"), part of the World Bank; the Overseas Private Investment Corporation ("OPIC"), an American governmental agency that insures certain American investments abroad; and Export Credits Guarantee Department ("ECGD"), a United Kingdom governmental agency that works specifically with British entities working abroad or British entities with investments abroad.[19] MIGA, OPIC, and ECGD use their own forms. These policies provide special benefits to the policyholders backed by government entities that have access to a wide breadth of information and can use their power to prevent or minimize the insured's loss. The policies are likely to be a form policy and may offer coverage for a longer period of time (sometimes up to twenty years).

Political risk insurance policies procured through private entities have certain advantages however. For one, the private market insurers do not have the same eligibility requirements – e.g., the insured must be a citizen of the United States (OPIC), the United Kingdom (ECGD), or one of the MIGA member countries – as the public insurers. Private providers of political risk insurance may be more likely to consider changes to certain policy provisions. Many businesses also appreciate the fact that the purchased private market political risk insurance can be kept confidential, as opposed to policies with government or quasi-government providers.

Ultimately, what a political risk insurance policy covers depends on how the policy is drafted. Unlike other types of insurance policies, political risk insurance policies are more likely

---

[18] *See* Sandra Smith Thayer & Kirk Pasich, *Insuring Against Political Risks*, Oil & Gas Fin. J. (Apr. 2011); Cyril Tuohy, *Egypt Causes Price Spike for Political Risk Insurance*, Risk & Insurance (Feb. 7, 2011), http://www.riskandinsurance.com/story.jsp?storyId=533329908 (noting one of the industries most affected by the Egyptian demonstrations was the hospitality sector).

[19] *See generally* MIGA, http://www.miga.org/; OPIC, http://www.opic.gov/what-we-offer/political-risk-insurance; ECGD, http://www.ukexportfinance.gov.uk/.

to be "manuscripted," or tailored, to the needs of the company purchasing the policy. Companies may also decide to mix and match coverage, obtaining coverage for certain risks with official providers and coverage for other projects with private providers. If a company is opening a new hotel in a historically unstable region, it may consider purchasing political risk insurance to cover work in that region.[20] Likewise, if a company is working with a government it has not worked with before on a particular project, it may want to cover just that project.

Because of these wide variations, the pricing of the policies will likely be dependent on the scope of the project, policy period, and the risk associated with certain regions.[21] Similarly, because of the specialized nature of these types of policies, it is important to review the policy terms to ensure the policy accurately reflects the intended scope of coverage.

In some ways, political risk insurance coverage may overlap with coverage provided through other sources, for instance, through a first-party property policy. For example, political violence insurance may cover property damage as a result of a riot and the resulting losses due to business interruption. However, many property policies exclude coverage for terrorist attacks or war. These exclusions create a gap in coverage abroad that political risk insurance may fill. Accordingly, even if a company believes it is covered, it should explore these issues with their brokers to confirm what is and is not covered.

As with all policies, it is important for an insured company to provide notice of a claim or change of circumstances to its providers immediately. As the Arab Spring protests demonstrated, riots and protests can quickly escalate to violence and civil war that destabilizes an entire region. Similarly, when a political leader passes away, it can result in instability in a region that was once stable. A change of government may lead to actions to abrogate certain agreements or contracts. Providing prompt notice to insurers, in accordance with a policy's particular notice requirements, increases the likelihood of coverage being honored.

IV. WAGE-HOUR CLASS ACTION LAWSUITS AND COVERAGE UNDER EMPLOYMENT PRACTICES LIABILITY INSURANCE

The number of new wage-hour class action lawsuits has increased dramatically in recent years, with cases often involving companies in the hospitality industry.[22] In federal courts alone,

---

[20] *See* Marsh & Maplecroft, Political Risk 2012, http://maplecroft.com/media/v_maplecroft-23122010_112502/updatable/email/marsh/Political_Risk_2012_Poster_MARSH.pdf.

[21] *See* Cyril Tuohy, *Counterpoint: Political Risk Is a Crude Science*, Risk & Insurance (Dec. 17, 2012), http://www.riskandinsurance.com/story.jsp?storyId=533353003.

[22] *See, e.g.*, *Cracker Barrel Old Country Store v. Cincinnati Ins. Co.*, No. 11-6306, 2012 U.S. App. LEXIS 19161 (6th Cir. Sept. 10, 2012) (insurance coverage dispute related to class action suits filed by the EEOC against Cracker Barrel, a nationwide restaurant chain operating in 41 states); *Berkshire-Cranwell Ltd. P'ship v. Tokio Marine & Nichido Fire Ins. Co.*, No. 11-cv-30194-MAP, 2012 U.S. Dist. LEXIS 93635 (D. Mass. July 6, 2012) (insurance coverage dispute related to employee class action alleging the resort charged guests a "service fee" at the restaurants and spa that it kept for itself instead of turning the fees over to employees who performed the services); *Cadete Enters. v. Phila. Indem. Ins. Co.*, 30 Mass. L. Rep. 181 (Mass. Super. Ct. 2012) (insurance coverage dispute related to class action brought by wait staff of Dunkin' Donuts alleging violation of Massachusetts Tips Act).

more than 7,000 wage-hour lawsuits were filed in 2011, representing both a record high and a roughly 400 percent increase since 2000.[23] Most often the suits involve claims under state labor laws and, to a lesser extent, the Fair Labor Standards Act ("FLSA"). Such suits constitute a serious risk to any company, with the possibility of multimillion dollars in liability and significant costs to defend against the wage-hour lawsuits.

Fortunately, Employment Practices Liability ("EPL") insurance may provide some protection to insureds. Insurance companies, however, have vigorously contested coverage for wage-hour lawsuits. One of the primary objections to coverage is the fact that many EPL insurance policies contain exclusions that may bar coverage for violations of the FLSA or "*similar*" provisions [or laws] of any federal, state, or local law (referred to herein as the "FLSA exclusion").[24] Due to the rise in wage-hour lawsuits and insurers' resistance to paying claims under EPL policies, this paper includes a brief overview of the scope of EPL coverage, the FLSA exclusion, and some practical guidance to aid in procuring coverage for wage-hour lawsuits.

A. Scope Of EPL Coverage

EPL insurance provides coverage for claims arising out of the employment relationship and typically obligates an insurer to pay all "loss" resulting from an employment-related claim. This includes the payment of all damages, judgments, settlements, prejudgment interest, post-judgment interest, and defense costs subject to the language of the policy. In addition to covering traditional employment-related claims, such as those alleging sexual harassment, discrimination, or wrongful termination, an EPL insurance policy ordinarily also provides coverage for a wide array of claims falling within the broad concepts of "employment-related torts," "employment practice violations," "wrongful employment practices," or similar catch-all terms. Examples of the latter types of claims include those alleging "misrepresentation," "negligent supervision," or the "failure to adopt or implement adequate work place or employment policies and procedures." (whether written or oral). Wage-hour lawsuits commonly allege claims falling within the scope of such EPL coverage provisions. For example, wage-hour plaintiffs routinely also assert claims falling within the broad concepts of "employment-related torts" or "employment practice violations." Such claims should trigger coverage under an EPL insurance policy.

B. The FLSA Exclusion

The FLSA exclusion frequently included in EPL insurance policies bars coverage for wage-hour actions alleging violations of the FLSA or "*similar provisions* of any federal, state or local law." Insurers have argued that the FLSA exclusion, which may exist in various forms, eliminates coverage for all wage-hour claims under state laws serving a "similar" purpose as the FLSA. Policyholders, however, should be able to avoid the exclusion by showing that the plaintiffs' wage-hour claims are based on a state law that is *dissimilar* to the FLSA. In fact,

---

[23] *See, e.g.*, Jonathan A. Segal, *The New Workplace Revolution: Wage And Hour Lawsuits*, CNNMoney (May 29, 2012), http://management.fortune.cnn.com/2012/05/29/the-new-workplace-revolution-wage-and-hour-lawsuits.

[24] *See, e.g.*, *Cadete Enters.*, 30 Mass. L. Rep. 181 (emphasis added) (finding no coverage for wage-hour class action brought by wait staff of Dunkin' Donuts alleging violation of Massachusetts Tips Act, because the policy contained an FLSA or "similar" law exclusion).

many wage-hour plaintiffs file claims under state labor laws, rather than the FLSA, precisely because of the *differences* between the state and federal laws. For example, the California Labor Code requires employers to provide adequate meal and rest breaks, maintain adequate wage-hour recordkeeping, and provide prompt payment to discharged employees at the time of termination, subject to stiff penalties for non-compliance.[25] The FLSA does not include these provisions. Courts have recognized such distinctions and considered them significant in addressing coverage claims.[26] As a result, the traditional FLSA exclusion described should not bar coverage for wage-hour claims brought under distinct state labor laws, such as the California Labor Code.[27]

In addition, when wage-hour plaintiffs allege violations of both the FLSA and state laws, the FLSA exclusion should not necessarily bar coverage, because an insurance company with a duty to defend must pay for the defense of its policyholder whenever the allegations in the underlying complaint raise the mere possibility that a claim may ultimately be covered by the policy.[28] Thus, even where an FLSA exclusion may bar indemnity coverage for certain claims alleged under the federal statute, a policyholder may still be able to obtain full defense coverage in connection with the lawsuit (absent express allocation and reimbursement provisions in the policy), so long as the complaint includes at least one state law claim potentially covered by the policy.[29]

C. Practical Guidance For Procuring Coverage For Wage-Hour Claims

As indicated above, traditionally the FLSA exclusion barred coverage for wage-hour actions alleging violations of the FLSA or "similar provisions of any federal, state or local law." In recent years, however, certain insurance companies have started selling EPL insurance policies with revised FLSA exclusions that expressly bar coverage for claims under the FLSA

---

[25] Cal. Lab. Code §§ 512(a), 226, 202.

[26] *See Cal. Dairies Inc. v. RSUI Indem. Co*., 617 F. Supp. 2d 1023, 1039-47 (E.D. Cal. 2009) (FLSA "similar" law exclusion applied to some claims, but not to the company's failure to reimburse employees for costs related to uniforms, comply with itemized wage statement requirements, or pay wages due at termination.); *Ramirez v. Yosemite Water Co.*, 978 P.2d 2, 10 (Cal. 1999) ("By choosing not to track the language of the federal exemption and instead adopting its own distinct definition . . . , the [California Industrial Welfare Commission] evidently intended to depart from federal law and to provide, at least in some cases, greater protection for employees.").

[27] *See Cal. Dairies*, 617 F. Supp. 2d at 1026-27.

[28] *See Truck Ins. Exch. v. Vanport Homes, Inc.*, 58 P.3d 276, 281-82 (Wash. 2002) ("The duty to defend 'arises when a complaint against the insured, construed liberally, alleges facts which could, if proven, impose liability upon the insured within the policy's coverage.'" (citation omitted)); *see also, e.g., Woo v. Fireman's Fund Ins. Co.*, 164 P.3d 454, 459 (Wash. 2007) ("[T]he duty to defend is triggered if the insurance policy *conceivably covers* the allegations in the complaint." (emphasis added)).

[29] *See Nat'l Union Fire Ins. Co. v. Earl Scheib, Inc.*, Am. Arb. Ass'n Case No. 72-195-00415-11 (Oct. 30, 2001) (arbitrator held that insurer was obligated to pay all defense costs despite an FLSA exclusion, where at least some of the underlying claims were brought under California labor laws having no federal counterpart.

"and *any other law concerning wage and hour practices*."[30] The language of the latter provision is arguably much broader than the former provision and appears to be at least one insurer's attempt to foreclose coverage for wage-hour claims based on state law that is distinct from the FLSA, such as the California Labor Code.[31] As a result, companies purchasing EPL insurance should carefully examine the version of any FLSA exclusion in the policy offered by the insurance company. Policyholders who purchase EPL policies with the narrower exclusionary language will be in a better position to seek coverage for wage-hour lawsuits.

In sum, as outlined above, EPL insurance can provide businesses with critical protection against the substantial costs and liabilities associated with increasingly prevalent wage-hour lawsuits. Policyholders also are well advised to carefully examine any FLSA exclusion during the procurement of EPL insurance coverage. The key to obtaining coverage may rest on whether the policyholder can show that some claims are based on state law provisions that differ from the FLSA.

[30] *See, e.g.*, Zurich Specimen Employment Practices Liability Insurance Policy § IV.4(c) (emphasis added) (excluding coverage for claims under the FLSA "and any other law concerning wage and hour practices, including, but not limited to any **Claim** for off-the-clock work, failure to provide rest or meal periods, failure to reimburse expenses, improper classification of employees as exempt or non-exempt, failure to timely pay wages, conversions, unjust enrichment, or unfair business practices" (bold emphasis in original)), http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/employmentpracticesliability/employmentpracticesliabilityzurichcorporatepolicyspecimen.pdf; *see also Classic Distrib. & Beverage Grp., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV 11-07075 GAF (RZx), 2012 WL 3860597, at *2, *7 (C.D. Cal. Aug. 29, 2012) (court invalidated exclusion (based on failure to provide adequate notice to the insured of the terms of the exclusion) that insurer argued barred coverage for wage-hour claims; exclusion barred coverage for "'an alleged violation of responsibilities, duties or obligations imposed on an Insured under any Wage and Hour Law'" (quoting Policy)), *vacated*, 2012 WL 5834570 (C.D. Cal. Nov. 6, 2012) (vacated by granting joint application of the parties).

[31] The fact that insurers are taking steps to redraft the FLSA exclusion suggests that they recognize the potential for coverage under the prior language.