LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 30, Number 2 • May 2015

DE Chancery Enjoins Board in Potential Stockholder Dilution Scheme

By Brett M. McCartney

Directors and officers of struggling corporations seeking capital or startups willing to trade equity for cash should carefully read the Delaware Court of Chancery's recent transcript ruling in *Elite Horse Investments Ltd. v. T3 Motion*, C.A. No. 10550-CB (Del. Ch. Jan. 23, 2015), and consider it a cautionary tale. If control of a business can be purchased, sitting directors and officers should not be surprised when the new controlling stockholder or control group installs its own directors and replaces management. Moreover, directors and officers should think long and hard before attempting defensive measures aimed at protecting their positions or other entrenchment motives. As discussed below, the Court of Chancery will not hesitate in enjoining such conduct.

Background

Elite Horse Investments Ltd. (EHI) is one of a group of stockholders of T3 Motion Inc., a Delaware corporation headquartered in Costa Mesa, CA, that designs, manufactures and markets electric-motor-powered personal mobility vehicles. In or around December 2014, EHI and a group of seven others invested $6 million in T3 Motion in exchange for approximately

continued on page 10

Long-Awaited Guidance on L-1B Visa Category Released

By Ian Macdonald

The highly anticipated draft Policy Memorandum (L-1B Memo) addressing the qualifying criteria for the L-1B visa category was released by U.S. Citizenship and Immigration Services (USCIS) on March 24, giving immigration practitioners and employers clear guidance on the definition of "specialized knowledge" and the standard of review USCIS adjudicators should apply when evaluating L-1B petitions. Corporate counsel should be prepared to address the qualifying criteria outlined in the L-1B Memo, which clarifies and expands on previous agency guidance regarding L-1B visa adjudication. The feedback period for the L-1B Memo ends on May 8 and becomes effective on Aug. 31.

Background

The L-1 visa, also known as the intracompany transferee visa, is a nonimmigrant visa classification that allows companies to transfer employees from a related foreign entity to a U.S. company. This visa category has two formats: the L-1A visa for transfer of executive and managerial personnel, and the L-1B visa for transfer of specialized knowledge personnel.

To qualify for an L-1B visa, an employee must possess, among other things, "specialized knowledge." USCIS regulations define this as "special knowledge possessed by an individual of the petitioning organization's product, service, research, equipment, techniques, management, or other interests and its application in international markets, or an advanced level of knowledge or expertise in the organization's processes and procedures." Many of the issues in current L-1B adjudications surround how this definition is applied in practice, and what a USCIS officer will actually consider to be "specialized."

The burden of proving that an individual has specialized knowledge, and further proving that the individual will use that knowledge in the U.S. role, rests solely on the petitioning company. This is an inherently challenging process as USCIS officers often have little or no knowledge of the company's operations and

continued on page 2

In This Issue

L-1B Visa Guidance 1

Stockholder Dilution 1

Puffery 3

Cyber Threats...... 5

Communicable Diseases 7

L-1 Petitions

continued from page 1

what knowledge may be specialized in their particular industry.

Current State and Challenges of L-1

Congress created the L-1 visa program to allow expedited transfer of employees within the same company. Currently, many employers are finding that the L-1B program has become arduous, arbitrary and unreliable. L-1B filings are under increased scrutiny by USCIS. Specifically, USCIS has issued an increasing number of requests for additional evidence (RFE) and denials. According to the National Foundation for America Policy March 2015 brief, in FY 2014 for L-1B petitions there was a 35% denial rate and a 45% RFE rate. As a comparison, in FY 2006 there was a 6% denial rate and a 9% RFE rate.

The National Foundation for America Policy March 2015 brief also found that Indian nationals have a 56% denial rate versus a 13% denial rate for all other non-Indian nationals. In addition, the March 2015 brief noted that L-1B extensions receive more denials than new L-1B petitions. These findings appear to be the result of change in USCIS L-1B adjudication policy that has not been officially implemented. Many Indian nationals have STEM degrees and are employed in the software engineering field, which USCIS appears to be holding to an arbitrarily high specialized knowledge threshold. In addition, because the L-1B standard has changed over time, cases that were easily approvable several years ago when the initial L-1B was filed are experiencing challenges with the L-1B extension.

In practice, employers receive an RFE on a majority of L-1B filings. The RFE is typically eight pages long and contains a laundry list of items and supporting documents to show that the candidate qualifies for the L-1B visa category. In many instances, the RFEs appear to be more similar to O-1 extraordinary ability standards than specialized knowledge standards. As a result, many companies choose to file L-1B petitions under the Corporate Blanket L (which is done at a U.S. Consulate or Embassy abroad) where possible or avoid L-1Bs altogether and pursue alternative nonimmigrant visas such as H-1B, TNs, O-1s, etc., or choose to transfer the employee to another country.

Ian R. Macdonald is a shareholder in the Business Immigration & Compliance Practice Group at international law firm Greenberg Traurig. He can be reached at macdonaldi@gtlaw.com.

Clearer Guidance

The L-1B Policy Memorandum provides some clearer guidance for employers using the L-1B visa program that addresses many of the challenges described above. First, the L-1B Memo asserts that, when adjudicating L-1B petitions, USCIS officers must apply a "preponderance of the evidence standard," by which an employer must show that it is more likely than not that the employee is eligible for the benefit sought. The L-1B Memo expressly rejects higher standards such as "clear and convincing evidence" or "beyond a reasonable doubt" that some USCIS officers apparently apply when reviewing L-1B petitions. In particular, the L-1B Memo states:

> Even if the officer has some doubt about a claim, the petitioner will have satisfied the standard of proof if he submits relevant, probative, and credible evidence, considered 'individually and within the context of the totality of the evidence,' that leads to the conclusion that the claim is 'more likely than not' or 'probably' true.

In addition, the L-1B Memo confirms that L-1B extensions should not as a matter of course be subject to heightened scrutiny by USCIS officers. For L-1B extensions involving the same underlying facts, the L-1B Memo instructs officers to give deference to the prior USCIS determination. Re-examination of a case

continued on page 9

The Corporate Counselor®

EDITOR-IN-CHIEF .... Adam J. Schlagman
EDITORIAL DIRECTOR .... Wendy Kaplan Stavinoha
MARKETING DIRECTOR .... Jeannine Kennedy
GRAPHIC DESIGNER .... Evelyn Fernandez

The Corporate Counselor® (ISSN 0888-5877) is published by Law Journal Newsletters, a division of ALM. Telephone: (877)256-2472
Editorial e-mail: wampolsk@alm.com
Circulation e-mail: customercare@alm.com
Reprints: www.almreprints.com

The Corporate Counselor P0000-233
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to:
ALM
120 Broadway, New York, NY 10271

Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, PA 19103
www.ljnonline.com

Insights. Innovation. Connected.

The Greatest Article Ever Written on Puffery!

By R. Scott Oswald and Adam Augustine Carter

There is a moment in the modern Christmas film classic "Elf" in which the titular character, a full-grown man who believes himself to be an elf from the North Pole, enters a seemingly run-of-the-mill coffee shop in New York City after passing what most would consider a forgettable neon sign on the facade of an equally forgettable storefront boasting "world's best cup of coffee." The "elf" runs into the shop and excitedly shouts to everyone in the shop, "You did it! Congratulations! World's best cup of coffee! Great job everybody!" The employees and patrons in the shop simply gaze at the display of enthusiasm with befuddled expressions.

Although this moment in the film is likely intended to show the viewer the comic extent of the character's naiveté, it perhaps unwittingly provides a perfect demonstration of the precarious relationship between a company's boasting and the potential impact on those to whom it crows. In the parlance of the law, communication of this type has come to be known as "puffery." The word "puffery" is a gem of the judicial lexicon. It is one of those rare words that holds enough legal significance to bring down major corporations, but sounds altogether silly when used in conversation. The brilliance of it lies in the fact that its silliness makes it a unique word, ripe for molding through the legal process.

R. Scott Oswald is the managing principal and **Adam Augustine Carter** is a principal of The Employment Law Group, P.C., based in Washington, DC. Mr. Oswald handles all manner of employment discrimination cases, including those litigated under Title VII and the Fair Labor Standards Act. Mr. Carter works closely with clients who suffer discrimination or retaliation under civil rights and whistleblower laws.

Puffery and the Law

Though the puffery concept's roots lie in contract law, the passage of the Dodd-Frank Act and the strengthening of the nation's efforts to stop securities fraud has increased the importance of puffery as a part of the legal vernacular of business. Puffery exists somewhere between basic claims about a product's qualities, and outright lies about the same product. In a publicly traded corporation, landing on the wrong side of the line can result in liability for securities fraud. The question then, is when does puffery cross the line into fraud?

Cases on "puffery" tend to hinge on what is reasonable for a consumer to believe, or in the investor context, what is reasonable for a company spokesperson to say.

Cases on "puffery" tend to hinge on what is reasonable for a consumer to believe, or in the investor context, what is reasonable for a company spokesperson to say. These are distinct ways to analyze the same concept, but ultimately each comes down to the kinds of evidence needed to demonstrate the other party's knowledge and intent.

Thankfully for the cheeky-but-bold proclamation that forms the title of this piece, interpretations of what is and is not puffery have repeatedly coincided with interesting pop culture vignettes to allow for what may actually be the greatest article ever written on puffery.

Jet Puffery: Contract Roots In *Leonard v. Pepsico*

One of the most famous uses of the term "puffery" comes from the case of *Leonard v. Pepsico, Inc.*, 88 F.Supp.2d 116 (S.D.N.Y. 1999), aff'd 210 F.3d 88 (2d Cir. 2000). The case is one now widely read by law students in contracts classes in part because it demonstrates the perils of unintentionally making a contract offer and in part because it is notoriously entertaining. The case grows from a 1990s-era promotional campaign by Pepsi, in which one could earn "Pepsi Points" by purchasing Pepsi products, and exchange those points for "Pepsi Stuff" from a catalog, including clothing, accessories and furniture. One of the commercials for the promotion, clearly targeted at a young audience, featured a young man donning Pepsi-branded merchandise, with a pause at various intervals to show the cost in Pepsi points for each item. The young man proceeds to fly to school in a Harrier jet, and in the landing process, he wreaks minor havoc on the school grounds. He touches down on the schoolyard, opens the cockpit, and quips, "Sure beats the bus." Here the commercial once again pauses to indicate that the jet costs 7 million Pepsi points. Inevitably, someone in "real life" managed to acquire 7 million Pepsi Points, and proceeded to attempt to order a Harrier jet by writing it into the catalog's order form. Pepsi's failure to provide the jet prompted the suit.

While the opinion is as famous for Judge Kimba Wood's description of the commercial and breakdown of the humor as it is for its jurisprudence on the subject of contract offers, it is discussed here because it states that "a reasonable viewer would understand such advertisements as 'mere puffery,' not as statements of fact … and refrain from interpreting the promises of the commercial as being literally true." Ultimately, the humorous nature of the commercial, combined with the $23 million cost of a real Harrier jet led the court to find that a reasonable person would not believe that the commercial constituted an offer.

Here, the puffery distinction saved Pepsico approximately $23 million — no meaningless sum,

continued on page 4

Puffery

continued from page 3

even to a company the size of Pepsico. Had the commercial been less clearly intended to be a joke, or had the number of Pepsi points jokingly suggested to purchase a Harrier jet been more in line with the actual cost of the jet, the case presumably could have come out differently.

Battlefield Puffery: The Modern Investor Application in *Kelly v. Electronic Arts, Inc.*

Fast forward 15 years to 2014. In the interim, a massive economic crisis occurred reverberating in a public outcry for legislation. Congress thereafter sought to strengthen the SEC's enforcement mechanisms via the Dodd-Frank Act, and created and implemented a statute that provides a reward for those who report publicly traded corporations that mislead investors. Though the concept of puffery has its roots in contract law, it has developed newly sharpened teeth in the realm of financial regulation and litigation. A publicly traded company's communications with its investors must now be careful not to step over the line from puffery into outright falsehood.

Like Pepsico, the the case of *Kelly v. Electronic Arts, Inc.*, 2014 WL 5361641 (N.D.Cal.), *7 (N.D.Cal., 2014), touches on matters related to popular culture. In 2013, the latest installment of EA's popular video game series "Battlefield" launched with a number of technical problems. The game's technical failures frustrated customers and incurred the online wrath of the notoriously unforgiving video game enthusiast commentariat. Reviews for the game were generally bad, and sales were significantly weaker than expected for a game that was well known to be one of EA's biggest moneymakers.

Of course, poor product launches and weaker-than-expected sales are not normally the basis for a lawsuit. Indeed, the suit is based not the poor launch, but EA's confident statements in advance of the launch that it had taken the proper precautions to prevent such a bug-riddled product landing on store shelves. EA indicated that it had worked closely with Microsoft and Sony, manufacturers of the primary devices on which Battlefield would run, to ensure that bugs were minimal. It also stated repeatedly that it had "de-risked" the game's code, and even referred to previous problematic entries in the series to indicate that it was "not going to repeat that mistake." After the buggy launch and general perception of market failure, EA's investors brought suit

This is more than a law school lesson in subjective versus objective analysis; the lesson here is related to evidence.

claiming that EA had in fact repeated its mistakes, and misled investors into providing support for those repeated failures.

Again, the judge found the statements to be puffery, and not misstatements of fact. Using a rubric developed in a previous California case, the *Kelly* court noted that "[a] projection of optimism or statement of belief is a 'factual' misstatement … if: 1) the statement is not actually believed; 2) there is no reasonable basis for the belief; or 3) the speaker is aware of undisclosed facts tending seriously to undermine the statement's accuracy. *Id*. at *7 (quoting *Kaplan v. Rose*, 49 F.3d 1363, 1375 (9th Cir.1994)).

The Takeaway: Specificity, Knowledge, And Reasonableness

The takeaway then, is that in the investor communications context, one of the most important distinctions between non-actionable puffery and a sort of unreasonable, actionable puffery is the knowledge of the speaker. What might ordinarily be run-of-the-mill puffery can be transmogrified into large scale liability for a company where the company representative knows what he or she says is not reasonably supportable. Unlike in *Leonard*, where the focus was on the reasonable interpretation of a message that a cola company was actually offering a sensitive military aircraft for seven figures in Pepsi points, the *Kelly* case focuses on the reasonableness of the speaker given the speaker's knowledge of facts not known to the recipient.

This is more than a law school lesson in subjective versus objective analysis; the lesson here is related to evidence. While the cases described above both lead to findings of puffery, with different evidence, the cases may have turned out differently. In *Kelly* in particular, the evidence would have benefitted from greater specificity, given that "[r]epresentations about forecasts are material to a reasonable investor, and may constitute material representations when they are sufficiently specific. For example … statements that defendants were optimistic about future growth in the market for a *particular product* were material. … " *S.E.C. v. Loomis*, 969 F. Supp. 2d 1226, 1236 (E.D. Cal. 2013) (citations omitted, emphasis added). As further demonstration, the same court found that statements involving specific interest rate returns on financial products were sufficiently specific to overcome an assertion that corporate statements were simply puffery or corporate optimism. *Id*.

This is consistent with our own practice. When approaching the SEC and Justice Department officials with a case under the Dodd-Frank Act's investor protection provisions, the questions a plaintiff must answer are primarily related to two things: materiality (is the alleged statement actually important to an investor's decision-making process?) and scienter (did company officials have reason to believe the statements were false or misleading?).

continued on page 10

Deritivative Cyber Litigation

Mitigating Exposure

By James D. Gassenheimer and Lara O'Donnell

Potential liability for data breaches has emerged as a major concern for businesses in the past few years as massive cyber-attacks are increasing, with companies that use or store private customer data electronically or use social media as part of their marketing strategy being the prime targets. These data breaches have contributed to an increase in director and officer (D&O) litigation in connection with cyber incidents, and will continue to do so, with plaintiffs seeking to capitalize on D&O policies that do not contain cyber or data breach exclusions.

The market for D&O cyber coverage is evolving in response to these issues. However, existing policies and those covering prior policy periods do not reflect current market trends. Many D&O policies connected to the current influx of D&O litigation lack cyber liability exclusions. Thus, although both businesses and insurance companies are responding to changes in cyber liability exposure and litigation, plaintiffs continue to capitalize on the possibility of payouts for cyber liability under D&O policies.

The Increasing Threat Of Cyber Intrusions and Data Breach Exposure

Various agencies, departments and organizations continue to take serious steps toward electronic data protection in recognition of emerging and evolving cyber threats. For instance, on Feb. 3, 2015, the Financial Industry Regulatory Authority (FINRA) released its Report on Cybersecurity Practices, focusing on cybersecurity issues within the financial services industry. *See* News Release, at http://tinyurl.com/kn7ezhj. Among its findings, FINRA notes that the frequency and sophistication of cyber-attacks continues to increase. *See* FINRA Report, http://tinyurl.com/n3ktz2n. With respect to broker-dealers, FINRA advises that the industry as a whole "must make responding to these threats a high priority." *Id*. FINRA reports that a variety of factors are driving exposure to cybersecurity threats, including advances in technology, changes in business models, and changes in how businesses and their customers use technology to create vulnerabilities in information technology systems. The tools used to access private information are increasingly sophisticated, and insiders may also pose a substantial threat.

Notably, the OCIE Summary indicates that most of the examined firms reported that they had been the subject of a cyber-related incident.

The Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) also released a cybersecurity examination sweep summary in February 2015, which examined 57 broker-dealers and 49 registered investment advisers concerning how they address the legal, regulatory and compliance issues associated with cybersecurity. *See* OCIE Cybersecurity Summary, http://tinyurl.com/kwcmuu4. Notably, the OCIE Summary indicates that most of the examined firms reported that they had been the subject of a cyber-related incident. A majority also stated that they experienced cyber-attacks directly or through one or more of their vendors. Most of the cyber incidents were related to malware and fraudulent e-mails.

On Feb. 13, 2015, the White House convened a summit on cybersecurity and data protection. *See* President Obama Speaks at the White House Summit on Cybersecurity and Consumer Protection, The White House Blog (Feb. 13, 2015), http://tinyurl.com/m3k4ers. President Obama noted that more than 100 million Americans had personal data compromised in recent data breaches, underscoring the importance of addressing the unique and often widespread risks associated with cyber intrusions.

Cybersecurity Litigation And the Undefined Standard of Care

Due to the increasing occurrence of data breaches, cyber litigation, including related D&O lawsuits, is on the rise. The FTC, for example, has initiated cybersecurity lawsuits and investigations. *See, e.g., FTC v. Wyndham Worldwide Corp.*, No. 13-1887 (ES), 2014 WL 2812049 (D.N.J. June 23, 2014) (FTC alleges Wyndham entities violated FTC act by failing to maintain reasonable and appropriate data security for consumers' sensitive personal information); *FTC v. Wyndham Worldwide Corp. (Wyndham II)*, 10 F. Supp. 3d 601 (D.N.J. 2014). The district court's denial of Wyndham's motion to dismiss the complaint in *Wyndham II* is presently before the Third Circuit Court of Appeals on interlocutory review, where the court will consider the FTC's authority to address cybersecurity issues under Section 5 of the Federal Trade Commission Act, as well as Wyndham's alleged cybersecurity lapses.

The FTC's brief cites the reasonableness standard articulated by the New Jersey district court, stating that reasonableness is the "touchstone" of the analysis. Brief for the Fed. Trade Comn'n (Nov. 5, 2014), http://tinyurl.com/k9uchjb. However, what constitutes "reasonableness" remains largely undefined by courts.

The FCC is also doubling down on cybersecurity. On Oct. 24, 2014, the FCC levied its first fine under the Communications Act of 1934, and ruled against two companies for failing to adequately protect

continued on page 6

James D. Gassenheimer is a partner and **Lara O'Donnell** is an associate on Berger Singerman's Dispute Resolution Team in Miami.

Cyber Threats

continued from page 5

consumer information. *See In the Matter of TerraCom, Inc. and YourTel America, Inc.*, FCC 14-173, Notice of Apparent Liability for Forefeiture (Oct. 24, 2014), http://tinyurl.com/lz7bmlz. The FCC imposed a fine of $10 million on the companies for failure to employ reasonable data security practices, misrepresenting to customers that appropriate technologies were used to protect their personal information, failing to properly protect customer information, and failing to fully inform customers that their personal information had been compromised by third-party access. *Id*.

The FCC noted that "consumers applying for telecommunications services have a reasonable expectation that the carrier will protect confidentiality" of personal information they provide in connection with a transaction. *Id*. at 8. It found that the companies' data security practices were "unjust and unreasonable" because they "failed to employ even the most basic and readily available technologies and security features" for protecting consumer information. *Id*. at 12.

Although case law and enforcement actions have yielded factual scenarios from which companies may discern particular practices that may not be appropriate, a uniform or better-defined standard of care has yet to emerge.

The Related Increase In D&O Litigation

Along with the proliferation of cyber litigation, related D&O lawsuits continue to present themselves in connection with data breaches. These lawsuits may seek to capitalize on D&O policies that lack specific cybersecurity exclusions. It remains unclear whether and to what extent traditional D&O policies would cover such claims. Standard D&O policies simply may not contemplate the new financial risks brought about by cyber liability and therefore may not adequately cover such claims. *See, e.g.*, Willis Warns Directors D&O Policies May Not Cover Some Cyber Risks, *Insurance Journal* (Aug. 6, 2012) (citing Willis Group Holdings Executive Risks Boardroom Guide). However, the steady increase in D&O lawsuits indicates that D&O plaintiffs may hope or expect to resolve those questions in favor of coverage under more traditional policies still in force. Because such policies are unlikely to contain cybersecurity exclusions, they may cover losses resulting from data breach-related derivative litigation.

The *Wyndham* case is one example of derivative litigation that arose in connection with a cyber-attack. In *Palkon v. Holmes*, No. 2:14-CV-01234 (SRC), 2014 WL 5341880 (D.N.J. Oct. 20, 2014), shareholders filed a derivative lawsuit against directors and officers of Wyndham Worldwide Corp. (Wyndham). The New Jersey federal district court dismissed the D&O case with prejudice on grounds that the plaintiff shareholder failed to show that the Wyndham board's demand refusal was made in bad faith or was based on an unreasonable investigation. Under the strong presumption afforded by the business judgment rule, the court found that Wyndham's board "had a firm grasp of Plaintiff's demand when it determined that pursuing it was not in the corporation's best interest." *Palkon*, 2014 WL 5341880 at *6. The court noted that the company had implemented cybersecurity measures before the first breach, and those measures were followed. This finding prevented the plaintiff from showing gross negligence.

Along with the proliferation of cyber litigation, related D&O lawsuits continue to present themselves in connection with data breaches.

A pair of derivative suits filed Jan. 21 and Jan. 29, 2014, over Target's data breach also remain pending in the federal district court for the District of Minnesota. The first complaint alleged breach of fiduciary duty and waste of corporate assets. *See Kulla v. Steinhafel*, Case No. 0:14-cv-00203 (D. Minn. Jan. 21, 2014). The second complaint alleged breach of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control. *See Collier v. Steinhafel*, Case No. 0:14-cv-00266 (D. Minn. Jan. 29, 2014). Both complaints alleged failure to take adequate steps to prevent a security breach, and that defendants "aggravated the damage to customers by failing to provide prompt and adequate notice to customers and by releasing numerous statements meant to create a false sense of security to affected customers."

Thus, D&O lawsuits have been cropping up in connection with major cyber litigation, and the frequency and severity of these lawsuits can be expected to grow. *See, e.g.*, D&O Claims & Trends Q2 2013, Advisen Insurance Intelligence (July 2013), http://tinyurl.com/l8cs9qe (expectations are that the frequency and severity of D&O suits will grow due to increased regulatory scrutiny); *see also* See Cyber Liability — the Changing D&O Risks, *WGA insureblog* (Oct. 10, 2014), http://tinyurl.com/mpljz49 ("The rise of cyber liability is threatening to cause one of the D&O insurance industry's periodic spasms.").

Mitigating Exposure To D&O Litigation

Existing case law does not clearly explain what constitutes "reasonable" precautions taken by a business. In *Wyndham*, the court offers some suggestions that guide compliance, noting that the FTC's public complaints and consent agreements, as well as its public statements and business guidance brochure, *see* FTC, Protecting Personal Information: A Guide for Business (November 2011), http://tinyurl.com/77jv,

continued on page 12

Communicable Diseases

What's an Employer to Do?

By Veena A. Iyer, Sarah Riskin and Elizabeth Winchell

In the past year, communicable disease outbreaks have dominated the headlines. Ebola arrived in the United States last fall; measles resurged this winter; and this year's influenza strains were some of deadliest in recent memory. In light of these public health threats, employers are struggling to ascertain their rights and obligations toward their workforce, including those who are infected, exposed, or at-risk.

What Is a Communicable Disease?

Communicable diseases are medical conditions that can be passed from one person to another. They vary widely in severity, ranging from minor illnesses like the common cold to acute conditions like Ebola. Communicable diseases also differ in method of transmission, with some conditions like influenza being transmitted through contact with an infected person or surface, and other conditions like tuberculosis being transmitted without any such contact.

Because of the differences among various communicable diseases, a "one-size-fits-all" formula is of little utility in dealing with concerns in the workplace. Rather, an employer should develop a flexible approach that can be applied to a variety of scenarios involving different communicable diseases. In doing so, the company should take into consideration laws that apply to employers generally and to the industry particularly and characteristics that are unique to the employer's workplace, workforce, and customers.

Veena A. Iyer is a shareholder in the labor and employment group at Nilan Johnson Lewis PA. **Sarah Riskin** and **Elizabeth Winchell** are associates at the firm, Riskin in the labor and employment group and Winchell in the health care group.

Which Laws Are Likely to Be at Issue?

When considering what actions can be taken to prevent or contain a single incident or a widespread outbreak of communicable diseases, employers should keep in mind a number of laws.

1. The Family and Medical Leave Act (FMLA) and any state medical leave statutes. These statutes require covered employers to provide qualified employees with leave to cope with the employee's own or a family member's medical condition. Under the federal FMLA, a covered employer must provide qualifying employees with 12 weeks of unpaid leave for their own or a family member's "serious health condition." Thus, to determine whether a qualifying employee is entitled to FMLA leave due to a communicable disease, the employer must assess whether the disease at issue amounts to a "serious health condition."

This is generally a case-by-case determination. The FMLA regulations define a "serious health condition" as "an illness, injury, impairment or physical or mental condition that involves inpatient care or continuing treatment by a health care provider." Employers should be able to evaluate fairly easily whether an employee meets the "inpatient care" prong, but will likely face more difficulty assessing whether an employee is receiving "continuing treatment." Generally, an employer or an employee's family member is receiving continuing treatment if he or she has been unable to work for at least three consecutive days, and has received a minimum amount of treatment from a medical provider.

In short, a bout of influenza that lasts a day or two and does not require hospitalization or treatment by a medical provider is not a "serious health condition" under the FMLA. But a case of influenza that requires hospitalization or lasts at least three days and requires treatment by a medical provider would likely qualify as a "serious health condition." Regardless of whether the communicable disease at issue qualifies as a "serious health condition" under the FMLA, employers should be sure to check whether the employee would be entitled to leave under any more generous applicable state or local law.

2. The Americans with Disabilities Act (ADA) and state disability anti-discrimination statutes. These statutes are designed to prevent discrimination on the basis of disability. Under the ADA, a covered employer is prevented from making disability-related inquiries or medical examinations except under certain circumstances and discriminating against qualified employees with actual or perceived disabilities. Employers also have the affirmative duties to provide reasonable accommodations to qualified employees with actual disabilities and maintain confidentiality of an employee's medical information. The Equal Employment Opportunity Commission (EEOC), the federal agency in charge of enforcing the ADA, has issued guidance to assist employers in applying the ADA to outbreaks of communicable diseases, particularly pandemics.

The ADA prohibits employers from making disability-related inquiries or conducting medical examinations of their employees, unless doing so is job-related and consistent with business necessity. This means the employer must have a reasonable belief, based on objective evidence, that the employee's ability to perform essential job functions will be impaired by a medical condition or that an employee will pose a direct threat due to a medical condition. Note that there are different rules for applicants, which is outside the scope of this article.

In light of these mandates, whether an employer makes a disability-related inquiry or requires a medical examination of an employee who may have been exposed to a communicable disease likely turns on the nature of the objective evidence regarding exposure, the characteristics of the disease, and the nature of the workplace. If a teacher at a

continued on page 8

continued from page 7

daycare center revealed that she was at Disneyland when visitors were exposed to the measles, an employer would likely be justified in requesting the employee undergo tests to confirm whether she is immune to the disease. In contrast, an employer would likely have greater difficulty requesting such testing of a law firm paralegal who traveled on a plane from Los Angeles in the days after the measles outbreak. In that case, the employer would lack objective evidence that the paralegal posed a direct threat because of her potential exposure to the measles.

The ADA also prohibits employers from discriminating against qualified employees who are disabled or who are perceived to be disabled. In the case of an employee who has a communicable disease, the initial question for the employer is whether that employee is disabled under the statute. Generally, a disability includes a condition that "substantially limits one or more major life activities," or "being regarded as" having a disability. Whether a communicable disease is a disability is therefore likely to depend on the severity of the disease in the particular case at issue. Influenza or H1N1 is unlikely to rise to the level of a disability, but measles or Ebola would probably amount to a disabling condition. Regardless of whether a communicable disease is a disability, it is unlikely that an employer would run afoul of the ADA by asking an employee who poses a direct threat to the health and safety of others. That said, the employer should consider offering telecommuting as a potential reasonable accommodation for an employee capable of working during the illness.

Finally, the ADA requires that information obtained through disability-related inquiries and medical examinations be kept confidential and stored separate from ordinary employment records. This prohibition raises the question of whether there is any way for employers to inform the workforce and the public about potential exposure to a communicable disease by an employee. In such situations, it is advisable to follow the guidance of the CDC and your jurisdiction of public health. Ordinarily, when employers do share such information, they do not reveal the identity of infected individual to whom others were exposed, but do provide enough information for those who were exposed to identify themselves and know to seek medical attention if they experience symptoms.

3. Title VII of the Civil Rights Act and state anti-discrimination statutes. These statutes prohibit discrimination on the basis of membership in various protected classes, including race, color, religion, gender and national origin. Employers should keep these statutes in mind when responding to a potential or actual communicable disease outbreak. Again, the more information an employer has about the disease and the outbreak, the better positioned the employer will be to protect the health and safety of the workplace while avoiding a claim of discrimination.

For example, during the Ebola outbreak last fall, a number of employers faced the question of whether they could and should prohibit employees who had traveled to certain West African countries from returning to work until the incubation period for Ebola had passed. Employers needed to be careful not to assume that their employees from West African countries were exposed to Ebola. Rather, the critical inquiry was whether an individual's travel placed him or her at higher risk for contracting and transmitting the disease. Employers were best served by educating themselves about the levels of Ebola in the countries that the employee had visited, obtaining information from the employee regarding any potential contact with infected individuals, consulting the guidance of their jurisdiction's public health department, and making case-by-case determinations about whether an employee should be sent home.

4. Federal and state reasonable accommodations requirements. Federal and state statutes, including the ADA and Title VII, require employers to make reasonable accommodations to non-essential employment functions and requirements for persons with disabilities and persons of faith. These accommodations are most likely to arise when employers seek to implement prevention programs, such as a mandatory vaccination program. Under these statutes, employers cannot force all employees to be vaccinated; rather, most employers will be required to exempt employees who are unable to be vaccinated because of a medical condition or who refuse to be vaccinated based on their religious beliefs. That said, the employer may take other steps to protect the employee, his or her coworkers, and the public, such as requiring the employee to wear a mask or ensuring that the employee is not exposed to particularly vulnerable populations.

Best Practices

- Institute a policy asking employees to stay away from the workplace if they are exhibiting symptoms of a communicable disease.
- If you ask employees to leave work if they are exhibiting symptoms, make sure to treat all employees consistently.
- Consider placing employees with or exposed to certain communicable diseases on paid leave or converting such employees to temporary work-at-home status.
- If you ask employees not to come to work or to leave work due to exposure, make sure that there is public health information regarding the spread and severity of the illness to justify this approach.
- Be aware of competing public health needs. If the employee must be quarantined, for example, do not take any adverse employment action as a result.

continued on page 9

Diseases

continued from page 8

- If your organization does not provide sick leave, consider doing so to avoid creating an incentive for employees to come to work sick.
- Review the EEOC's pandemic preparedness guidance when assessing how to handle a communicable disease outbreak.
- Be aware of industry-specific rules and regulations. For example, depending on the state, there may be special rules in food-handling, healthcare, hotels, public swimming pools, and school/day care settings.

—❖—

L-1 Petitions

continued from page 2

should only occur if there was a material error related to the initial L-1B approval, there has been a "substantial change in circumstances" since the approval, or there is new material information that adversely impacts the eligibility for the visa classification. This will help reverse the recent trend of USCIS approval rates being lower for L-1B extensions than for initially filed petitions.

The L-1B Memo provides some clarification of the definition of "specialized knowledge." It establishes that for knowledge to be "special" or "advanced," there must be a comparison of the beneficiary's knowledge against that of other workers. To be "special," the knowledge must be "distinct or uncommon" in comparison to that normally found in the employer/industry, whereas to be "advanced" the knowledge must be "greatly developed or further along in progress, complexity and understanding" than generally found within the employer. Factors USCIS will consider in determining whether a beneficiary's knowledge is specialized include:

- Whether the beneficiary possesses knowledge not generally found in the industry or the petitioning organization's U.S. operations.
- Whether the beneficiary possesses knowledge that is particularly beneficial to the employer's competitiveness in the marketplace.
- Whether the beneficiary has been employed abroad in a capacity involving assignments that have significantly enhanced the employer's productivity, competitiveness, image, or financial position.
- Whether the claimed specialized knowledge normally can be gained only through prior experience with that employer.
- Whether the beneficiary possesses knowledge of a product or process that cannot be easily transferred or taught to another individual without significant economic cost or inconvenience (because, for example, such knowledge may require substantial training, work experience, or education).
- Whether the beneficiary has knowledge of a process or a product that either is sophisticated or complex, or of a highly technical nature, although not necessarily unique to the firm.

The L-1B Memo also confirms that knowledge need not be proprietary or unique to the petitioning employer, or narrowly held within the petitioning employer to be "specialized," but such evidence would support a finding that the knowledge is specialized. Moreover, the L-1B Memo reminds USCIS officers that petitioners need not prove that U.S. workers are unavailable to perform the duties of the position. While it may be the case that a high number of U.S. workers possessing knowledge similar to beneficiary's can result in a conclusion that the beneficiary's knowledge is not "specialized," an employer is not required to prove the alternative.

The L-1B Memo makes clear that merely stating that a beneficiary's knowledge is different, special, or greatly developed is not sufficient to qualify for L-1B classification; the employer must submit proof. To that end, the L-1B Memo provides instructions to employers as to the kinds of evidence that can be submitted to USCIS to demonstrate that an individual's knowledge is "special" or "advanced." This evidence includes:

- A detailed description of the services to be performed;
- Proof of the beneficiary's prior education, training, and employment;
- A comparison of the beneficiary's knowledge to that of others;
- Proof of how and when the beneficiary gained the required "specialized knowledge";
- An explanation of the difficulty of imparting the beneficiary's specialized knowledge to others without significant cost or disruption to the employer's business;
- Documentation of training, work experience, or education establishing the number of years the individual has been utilizing or developing the claimed specialized knowledge as an employee of the organization or in the industry;
- Evidence of the impact, if any, the transfer of the individual would have on the organization's U.S. operations;
- Evidence that the alien is qualified to contribute to the U.S. operation's knowledge of foreign operating conditions as a result of knowledge not generally found in the industry or the petitioning organization's U.S. operations;
- Contracts, statements of work, or other documentation that shows that the beneficiary possesses knowledge that is particularly beneficial to the organization's competitiveness in the marketplace;

continued on page 10

L-1 Petitions

continued from page 9

- Evidence, such as correspondence or reports, establishing that the beneficiary has been employed abroad in a capacity involving assignments that have significantly enhanced the organization's productivity, competitiveness, image, or financial position;
- Personnel or in-house training records that establish that the beneficiary's claimed specialized knowledge normally can be gained only through prior experience or training with that employer;
- Curricula and training manuals for internal training courses, financial documents, or other evidence that may demonstrate that the beneficiary possesses knowledge of a product or process that cannot be transferred or taught to another individual without significant economic cost or inconvenience;
- Evidence of patents, trademarks, licenses, or contracts awarded to the organization based on the beneficiary's work, or similar evidence that the beneficiary has knowledge of a process or a product that either is sophisticated or complex, or of a highly technical nature, although not necessarily proprietary or unique to the petitioning organization; and
- Payroll documents, federal or state wage statements, resumes, organizational charts, or similar evidence documenting the positions held and the wages paid to the beneficiary and parallel employees in the organization.

Finally, the L-1B Memo also addresses offsite L-1 employment, where an employee works at non-employer worksite. It reaffirms the two-prong test stated in the L-1 Visa Reform Act: 1) the beneficiary is not "controlled and supervised principally by the unaffiliated employer"; and 2) the beneficiary is "placed in connection with the provision of a product or service for which specialized knowledge specific to the petitioning employer is necessary."

Conclusion

Corporate counsel should be sure to address these two prongs for any offsite L-1 petitions. They should also be aware of and avoid any co-employment challenges, such as where the non-affiliated employer provides guidance and direction to the L-1, provide an e-mail address to the L-1, invites the L-1 to company parties, etc., particularly during a year when 30,000 unannounced H-1B and L-1 employer site visits by USCIS officers are expected. Corporate counsel who understand the qualifying criteria outlined in the L-1B Memo will best position their companies for success.

—❖—

Puffery

continued from page 4

To use the *Kelly* case as an example, this means that had the plaintiffs been able to marshall evidence that EA had not actually worked with Microsoft or Sony in any meaningful capacity, that the game's developers had not taken significant efforts to "de-risk" the game's engine, or perhaps even that the bugs in the launch were substantially the same bugs in the previous iterations of the series, then the decision might have come out differently. This would mean that the statements were not simply "projections of optimism," but rather statements that the speakers had reason to believe were false.

These evidentiary lessons should be a guide in developing or defending cases like these going forward. The power of puffery has only expanded since the days when preening teenagers flew harrier jets to school. The concept has reached the litigation battlefield repeatedly, including through the virtual battlefield of … well, Battlefield.

continued on page 12

DE Chancery

continued from page 1

60 million shares or roughly 60% of T3 Motion's equity. At the time of EHI's investment, T3 Motion's board of directors was composed of three members: CEO William Tsumpes, Steven Healy and Ki Nam. However, T3 Motion's bylaws authorized the company to have seven directors on the board.

On Dec. 26, 2014, EHI and seven other T3 Motion stockholders, holding in excess of 60% of T3 Motion's shares, delivered a signed stockholder written consent dated Dec. 17, 2014, electing four individuals to T3 Motion's board, thus filling the four vacant director seats. In response, on Jan. 15, Tsumpes contacted Healy and Nam to hold a board meeting, excluding the directors appointed to the T3 Motion board by the December 2014 written consent. The tentative agenda of the board meeting included the "urgent" matter of selling T3 Motion equity to a third-party investor, converting T3 Motion debt held by Tsumpes and an entity called T-Energy to equity and converting Tsumpes' unpaid salary to common stock. The motive behind these actions was to dilute EHI's and the other seven investor stockholders' interests in T3 Motion to less than a controlling majority.

EHI initiated the underlying action Jan. 16, pursuant to Section 225 of the Delaware General Corporation Law, and sought a declaratory judgment that the new directors were validly elected. Around the time EHI filed its Section 225 action, the four "new" T3 Motion directors, along with existing director Nam,

continued on page 11

DE Chancery

continued from page 10

executed a written consent removing Tsumpes as CEO and appointing one of the new directors in his stead.

On Jan. 20, EHI and six other stockholders collectively holding approximately 58% of T3 Motion's stock issued a written consent dated Jan. 15 that ratified and retook the actions in the December 2014 written consent — and removed Tsumpes and Healy from the T3 Motion board of directors. On Jan. 21, EHI filed an amended complaint seeking declarations that the director consent and the second stockholder consent were also valid and enforceable. In addition, EHI filed a motion for a temporary restraining order seeking to enjoin the T3 Motion board of directors and Tsumpes from taking certain actions that could harm the company, including the dilution of T3 Motion's stock. T3 Motion opposed the motion on three bases. First, the defendant argued that the stockholders' consents ran afoul of Section 211(b) of the DGCL. Second, the defendant contended the consents failed to comply with the date and signature requirements of Section 228(c) of the DGCL. And third, the defendant alleged that EHI failed to comply with the prompt notice requirement in Section 228(e) of the DGCL when delivering the consents.

The Ruling

The court was unmoved by the defendant's argument that, pursuant to Section 211(b), the December 2014 stockholder consent was unlawful because, as a less than unanimous stockholder consent, the December 2014 stockholder consent did not remove all T3 Motion's directors before filling vacancies on the board. Rather, Chancellor Andre G. Bouchard indicated that Section 211(b) applies when a stockholder written consent electing directors purports to be in lieu of an annual meeting. Because the December 2014 stockholder consent did not intend to replace an annual meeting, Section 211(b) was inapplicable.

The court noted that Section 228 of the DGCL allows for written consents to be utilized in these circumstances unless otherwise provided in a company's charter. In fact, T3 Motion's bylaws include language permitting stockholders to take any action that is required or permitted to be taken at an annual or special meeting by written consent. The chancellor also noted that support for this position can be found in the relatively recent Delaware Supreme Court decision in *Crown EMAK Partners LLC v. Kurz*, 992 A.2d 377 (Del. 2010). Relying on *Crown EMAK*, the chancellor stated that a company's charter must be explicit in prohibiting stockholders from filling board vacancies by written consent. Clearly, that was not the case here. For those reasons, the chancellor found it reasonably probable that EHI would succeed on its argument that the consenting directors had the ability to appoint directors to the vacant board seats by written consent and that the Section 211(b) defense was without merit.

The court also dispatched the two technical defenses raised by the defendant. The first argument centered on the purported failure of the December 2014 written consent being properly signed and dated. The court found that regardless of the validity of the defendant's argument, it was subsequently mooted by the January stockholder consent, which there was no argument that it was properly signed and dated. The January stockholder consent both retook and ratified the December 2014 stockholder consent. Similarly, the court found no support for the defendant's final argument that T3 Motion was not given prompt notice of the consents consistent with Section 228(e). The defendant failed to identify any authority for the proposition that Section 228(e) requires notice in less than 30 days. Without any support for its untimely notice argument, the court found the defendant's Section 228(e) defense lacked merit. After sorting through the various defenses, the chancellor granted the motion for a temporary restraining order, noting that it was similar in nature to status quo orders that are customarily imposed in Section 225 actions.

'Plainly Irreparable Harm'

Of particular note, the chancellor stated that the uncertainty of the composition of T3 Motion's board of directors put a cloud over how the company would be managed, which is "plainly irreparable harm." The value in this statement, however, may be limited by the circumstances confronting the court. Since a majority of the T3 Motion board of directors (four of seven) were appointed by the disputed stockholder consents, irreparable harm to the company is more likely, since interim actions for the company would be taken by a minority of directors. Whether the same threat of imminent irreparable harm exists where a minority of the directors' seats are in dispute is debatable. Nevertheless, the Court of Chancery demonstrated, yet again, its willingness to act quickly and decisively in order to protect Delaware companies and their stockholders from potential harm.

—❖—

Brett M. McCartney (bmccartney@morrisjames.com) is a partner at Morris James in Wilmington, DE. He practices primarily in the Delaware Court of Chancery and Delaware Superior Court, and focuses on corporate governance and complex commercial litigation, stockholder litigation, fiduciary duties, alternative entity disputes, class action, and derivative litigation. This article also appeared in the *Delaware Business Court Insider*, an ALM sister publication of this newsletter.

Cyber Threats

continued from page 6

indicate reasonable measures to be taken with respect to cybersecurity. It further suggests that industry practices may guide the reasonableness inquiry. *Wyndham*, 10 F. Supp. 3d at 620. Various other regulatory agencies and organizations also offer guidance on protecting private information, including the SEC, FINRA, the National Association of County Information Officers (NASCIO), the U.S. Department of Homeland Security (DHS), and the Department of Justice (DOJ). *See* Mitigating the Threat of Cybersecurity Litigation in an Ambiguous Regulatory Environment, 57 No. 2 DRI For Def. 48 (Feb. 2015).

Development of industry standards would address some of these concerns. The February, 2015 FINRA Report notes that an effective practice for firms would be to evaluate industry frameworks and standards as reference points for developing their approach to cybersecurity.

The FINRA Report suggests a number of frameworks and standards that businesses may draw upon as a starting point, including the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 created pursuant to Executive Order 13549 of Aug. 18, 2010, among others. *See* NIST Framework (Feb. 12, 2014), http://tinyurl.com/o7z6u9e. The NIST Framework specifically calls for businesses and organizations to establish a roadmap for reducing cybersecurity risk that considers legal and regulatory requirements, industry standards and best practices, and reflects risk management priorities. The related NIST Roadmap for Improving Critical Infrastructure Cybersecurity, http://tinyurl.com/kwl8uhc, echoes that "industry groups, associations, and non-profits can be key vehicles for strengthening awareness of the Framework."

Another important step in mitigating cyber liability, and in particular, D&O liability, is to ensure adequate cyberinsurance coverage.

Cyberinsurance

Another important step in mitigating cyber liability, and in particular, D&O liability, is to ensure adequate cyberinsurance coverage. Insurers are well aware of the increasing risk of cyber liability for businesses. *See, e.g.*, Increased D&O Diligence Required, The Hartford, http://tinyurl.com/lyuwlgt; Cyber D&O claims may be on the rise, *Zurich Insider* (Jan. 2015), http://tinyurl.com/ln-l5w2e. Some have suggested that, rather than excluding cyber events, D&O insurers may ask more questions of boards to determine their role and duties with respect to cyber risk management. *See* Why Cyber Risk as a Boardroom Issue Can't be Ignored, WS&Co., http://tinyurl.com/l3zuh5o. However, it is becoming increasingly difficult for businesses and insurers to keep up with the many facets of cyber liability exposure. *See supra* Cyber Liability — the Changing D&O Risks (Oct. 10, 2014).

Conclusion

Cybersecurity risks are largely unknown and in constant flux. In addition to negotiating D&O policies that do not specifically exclude cyber liability, it is equally important to obtain an adequate scope of coverage. Coverage should address a broad range of cyber risks, such as third party or vendor exposures, regulatory liability, cybercrime, and other foreseeable costs to the business resulting from a cyber incident. To the extent possible, policies should also include language broad enough to cover some risk of exposure to undefined cyber threats. It is imperative that businesses and their advisers stay on top of evolving cyber risks to ensure that adequate coverage remains in place.

—❖—

Puffery

continued from page 10

The key is to watch for statements that are specific, to probe speakers based on their knowledge at the time they made their statements, and to shore up the message recipient's reasonableness in interpreting the message based on its context.

The statement that a coffee shop makes the "world's best cup of coffee" is self-evidently subjective and lacking in specificity (*e.g.*, best according to what authority?). The barista likely lacked any specific information suggestinvworld's greatest, and certainly had no reason to believe that the bold proclamation would be taken as literal truth. And, of course, Will Ferrell's iconic Elf character should be no one's model for reasonableness.

—❖—