the Corporate Governance Advisor

March/April 2015 • Volume 23, Number 2

CYBERSECURITY

Changing the Cybersecurity Playing Field in 2015

By Paul Ferrillo

If this incident [Sony] isn't a giant wake-up call for U.S. corporations to get serious about cybersecurity, I don't know what is. I've done more than two dozen speaking engagements around the world this year, and one point I always try to drive home is that far too few organizations recognize how much they have riding on their technology and IT operations until it is too late. The message is that if the security breaks down, the technology stops working—and if that happens the business can quickly grind to a halt. But you would be hard-pressed to witness signs that most organizations have heard and internalized that message, based on their investments in cybersecurity relative to their overall reliance on it."

—Author Brian Krebs, Dec. 20, 2014.[1]

For those worried that what happened to Sony could happen to you, I have two pieces of advice. The first is for organizations: take this stuff seriously. Security is a combination of protection, detection, and response.

Continued on page 2

Paul Ferrillo is a Partner of Weil, Gotshal & Manges LLP. A version of this article was initially distributed as a Weil client alert.

Wolters Kluwer

CONTENTS

CYBERSECURITY

Changing the Cybersecurity Playing Field in 2015 1
By Paul Ferrillo

INSIDER TRADING

The Boundaries for Insider Trading Prosecutions See a Resurgence: The 1980s Are Back! 7
By Marc D. Powers, Mark A. Kornfeld, Jonathan A. Forman, and Margaret E. Hirce

POLITICAL SPENDING

Responding to Corporate Political Disclosure Initiatives: Guide for In-House Counsel 12
By Robert Kelner, Bob Lenhard, Keir Gumbs, and Zack Parks

SHAREHOLDER PROPOSALS

***Trinity v. Wal-Mart*: Serious Implications for the Ordinary Business Exclusion** 17
By Keir Gumbs and Reid Hooper

EXECUTIVE COMPENSATION

The Many Governance & Cost–Savings Benefits of Mandatory Post-Vest Holding Requirements 21
By Laura Wanlass and Chris Fischer

DISCLOSURE EFFECTIVENESS

A Call for Relevant Proxy Redesign 24
By Elizabeth M. Dunshee and Alexis C. Hamilton

> You need prevention to defend against low-focus attacks and to make targeted attacks harder. You need detection to spot the attackers who inevitably get through. And you need response to minimize the damage, restore security and manage the fallout.
>
> —Professor Bruce Schneier, Dec. 19, 2014.[2]

Without a doubt, the last month in the world of cybersecurity has been tumultuous. It has now been confirmed that two companies in the United States have potentially been the subject of cyber-terrorism. Servers have been taken down or wiped out. Businesses have been significantly disrupted. Personally identifiable employee information has been shoveled by the pound onto Internet credit card "market" sites. The cybersecurity world has changed, and two of the most respected men in cybersecurity have both iterated similar messages: it is time for U.S. corporations to take this stuff seriously.

This alert does not aim to recount the parade of horribles of 2014; rather, I write to suggest three modifications that are highly achievable in the corporate world that have the potential to make our cybersecurity world a little bit better in 2015.

More Cyber Governance—More NIST Discussions—More Information Sharing

On the first day of Christmas, my true love gave to me: the NIST cybersecurity framework.

In reality, on February 12, 2014, the Obama Administration, through the National Institute of Standards (NIST), announced the NIST Cyber Security Framework to "allow organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure."[3] The Framework focuses US infrastructure companies on five basic principles:

(1) Describing their current cybersecurity posture,

(2) Describing their target state for cybersecurity,

(3) Identifying and prioritizing opportunities for improvement within the context of a continuous and repeatable process,

(4) Assessing progress toward the target state, and

(5) Communicating among internal and external stakeholders about cybersecurity risk.[4]

NIST focuses companies on two simple questions:

(1) where are they currently with cybersecurity, and

(2) where do they want to be in the future?

Even more elegant is the simple way the Framework steers conversations regarding the way a company should review its core processes of protecting its most precious intellectual property (IP), trade secrets, or customer information:

- **Identification**—Developing the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. In other words, what are the most prized IP assets, and where are they located, for example, offline servers, network servers, or the cloud?

- **Protection**—Developing and implementing systems to protect the company's most valuable IP assets.

- **Detection**—Developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event. An event may be nothing after it is appropriately investigated. An event that is missed or not apprehended as something more severe might turn into a catastrophic incident resulting in a mega-breach.

- **Respond**—Developing an Incident Response Plan.

- **Recover**—Developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[5]

A thorough reading of the history behind the Framework points to two conclusions:

(1) It was not meant to become the national standard for cybersecurity best practices in the United States (the Framework expressly says adoption of its principles is "voluntary," though many argue that it is already *de facto* a national standard being used by the government and its third-party vendors), and

(2) The Framework was designed so that executives and employees of any company could, using a common language, determine the "what, who, where, when, and how" to protect its most valuable intellectual property assets.

Though some take issue with the lack of specificity regarding implementation of the standard, I would argue that is the point. No company is the same. No IP is the same. Therefore, there is no one perfect method for protecting a company's data. But there was a need to help companies organize their discussions around cybersecurity in a way that could be used by all directors, officers, and employees, whether they are technologically savvy not, to better their cybersecurity posture and defenses. That is what the Framework is all about.

If the Framework has become at the very least a national standard for cybersecurity, however, then are companies actually using it to facilitate discussions aimed to better their cybersecurity posture? How often are they using it? Annually? Quarterly? Are they using it at all? If companies are not using the *de facto* national standard for cybersecurity, then why is that the case?

If companies are using the Framework, how are they documenting discussions concerning improving their cybersecurity posture? Or are they just not documenting their cyber-related discussions at all? Good cyber governance starts with information and discussion, traveling from bottom to top and then from top to bottom. There is no "run and hide" option here, as that could land a board of directors with a major cyber breach on its hands and no documentation to rely upon to show they exercised their fiduciary duties of oversight over the enterprise's risk management. It also could land the company in further hot water with the plaintiffs' bar, which is becoming ever more successful, requiring the company to prove it did as best it could regarding cybersecurity despite the fact that a hacker still accessed its network.[6]

More (and Better) Employee Training and Education

Employee cyber training and education concepts could themselves be the subject of any number of articles or books. I mention them here in an attempt to raise two points to consider:

(1) Employee phishing and spear phishing training is imperative.

Some of the most notorious espionage cyber campaigns against companies and industries have started from the most innocent-looking emails sent to an unsuspecting company employee or executive under the guise of an email from a bank or credit card company. When the employee unsuspectingly opens the email or its attachment, it drops malware on the company computer, which quickly spreads to the network. "Once on a system, the malware gathers information such as the operating system version, computer name, user name, and local IDs, as well as system drive and volume information. All the data that is collected is encrypted and sent to a cloud account … in an apparent attempt to avoid detection by anti-malware tools."[7] Then the hacker goes to work stealing the company's most valued business information, including business plans, merger and acquisition-related

information, consumer information, and personally identifiable information.[8]

This threat vector is called "phishing," or its more advanced cousin, "spear phishing,"[9] when an email "phishes" for an unsuspecting and usually innocent employee to inadvertently wreak havoc on a company by opening it. "91 percent of cyber-attacks start with spear phishing…."[10] "Phishing remains a very real threat to organizations of any size. Symantec research showing a 91% increase in spear-phishing attacks from 2012 to 2013 tells us that much."[11] Says another expert, "The pool of spear phishing targets in 2015 will be larger and not just limited to a select few, like executives…."[12]

Many companies train their employees monthly using random phishing emails aimed to look like they came from either the company itself or another trusted source. Training employees on anti-phishing techniques should lower the success rate of phishing emails. Indeed one study showed that in one company, "between 26% and 45% of employees at those companies were Phish-prone, or susceptible to phishing emails. Implementation of [training] immediately reduced that percentage by 75%; with subsequent phishing testing over four weeks resulting in a close to zero phishing response rate across all three companies."[13]

Training is a good idea. Investing in more training this year would be an even better idea.

(2) Employee intrusion detection training is also essential.

Many companies now employ a host of various intrusion detection devices to attempt to detect a cyber-intrusion. These devices generally collect reams and reams of information called "logs," which could contain evidence of either network anomalies or common host-based artifacts of data theft. These could include:

- Evidence of abnormal user activity;
- Evidence of login activity outside expected hours;
- Odd connection durations;
- Unexpected connection sources;
- Evidence of abnormally high CPU or disk utilization;
- Evidence of File Artifacts associated with the use of common compression tools; and
- Evidence of recently installed or modified services.[14]

These logs are obviously very long and complicated. Given that many data breaches have occurred on a company's servers long before they are discovered (an average of 229 days), and given that many of the high-end intrusion detection devices that companies are employing are very good technically, many argue that there is a perceived mismatch between man and machine.

I am not sure there is good answer to the man vs. machine question. Some intrusion detection systems are so sophisticated that many of the high-level examination and analytical work can be done automatically, saving time and effort chasing false alerts and highlighting potentially malicious activity. Others are not. I express no opinion other than *caveat emptor*.

Nevertheless, company employees should be thoroughly trained repeatedly about their intrusion detection systems so that false positives can be ignored and potential dangerous incidents can be identified. Many intrusion detection vendors offer such training routinely, and it should be taken advantage of at all levels, as the more time malware is on company servers, the more time there is for it to wreak havoc on the network.

A Table-Topped, Battle-Tested, Infantry-to-Board of Directors, Incident Response Plan

In previous alerts,[15] we have spoken at length about the value of Incident Response Plans (IRPs).[16] Here are some additional relevant facts:

- The Ponemon *2014 Cost of Data Breach Study: United States* reported that the average cost for each lost or stolen record was $195. However, if a company has a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced by as much as $17 per record. Appointing a chief information security officer (CISO) to lead the data breach incident response team reduced the cost per lost or stolen record by $10.[17]

  There has been much talk in the industry of the importance of a CISO. Though every organization has to make its own determination as to whether such a position is needed within its company, at the very least *someone* needs to be 100 percent responsible for network security issues. That role is often filled by the CISO.

  According to the previous statistics, a CISO often can be an incredible asset to any mid-size to large company. As noted in one recent retailer breach, the company "didn't have an advocate at the C-level, as an executive, advocating for IT security investment.… If [the company's] senior management had known of such risks and what was at stake, they would have 'made very different choices' as to how it structured its organization, and how it invested in capabilities to defend the company's data."[18]

- IRPs should be practiced *at least* once a quarter and the owner of the IRP (presumably the CISO) should update the plan as needed to account for new plans, new vendors, or new data protection strategies.

- IRPs should be practiced by everyone—from IT departmental heads, to CEOs, to board members—and should include vendors, forensic consultants, investor relations or public relations consultants and lawyers to make the training as real as possible. It's important to practice for the worst. If something less than that occurs, then everyone should be on the same page when the next incident happens. If something in the IRP doesn't work, then it would be good to know that beforehand, rather than during an actual data breach.

What to Do in 2015

For many companies, it is probably time to get serious. The events of December 2014 have proved that we have most likely entered into a new phase of cyber-intrusions, cyber-attacks, and cyber-terrorism. Our network perimeters have plenty of penetration points to attack. And the Emperor's New Clothes are showing.

The events of late 2014 will require a new round of discussions with boards of directors and their C-Suite executives about company cybersecurity policies and what companies can do to mitigate the cyber risks involved. The critical IP assets of a company need to be fully and completed identified and protected as best as possible, using a variety of strategies including virtualization and private cloud strategies. History has shown strong perimeter defenses are no barrier to a determined hacker. Board discussions must occur, changes and improvements need to be documented, and incident response plans (including provisions for the absolute destruction of data, not just theft or tampering) need to be reviewed, modified as necessary and practiced. At a minimum, companies can insure for some of their cyber risk exposures through cyber insurance. Network security takes a village, involving every employee of the company. A culture of security needs to be instilled in every person touching a keyboard or a keypad.

Additionally, as cyber breaches have impacted varying industries in the United States, each has come away with separate lessons to be learned from each event. Because not all malware is one-of-a-kind, information sharing would be incredibly helpful to all organizations. We cannot

defeat this problem alone. We need to work together in a public/private partnership to share threat information. In this vein, Congress should pass the Cybersecurity Information Sharing Act as soon as possible in the coming term.[19]

By using some of the strategies I outline above, we can hopefully do a better job this year protecting our companies, businesses, and employees.

We *need* to do better in 2015.

Notes

1. *See* "FBI: North Korea to Blame for Sony Hack," available at *https://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/*, last accessed Feb. 3, 2105.

2. Mr. Schneier, a security technologist, is a fellow at the Berkman Center for Internet and Society at Harvard Law School. His recent Op-Ed Essay in the *Wall Street Journal* is available at *http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701*, last accessed Feb. 3, 2015.

3. *See* "NIST Releases Cybersecurity Framework Version 1.0," available at *http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm*, last accessed Feb. 3, 2015.

4. *See* the Framework, available at *http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*, last accessed Feb. 3, 2015.

5. *Id. See generally,* "Understanding and Implementing the NIST Cyber Security Framework," available at *http://blogs.law.harvard.edu/corpgov/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/*, last accessed Feb. 3, 2015.

6. *See, e.g.,* "Banks' Lawsuits Against Target for Losses Related to Hacking Can Continue," available at *http://bits.blogs.nytimes.com/2014/12/04/banks-lawsuits-against-target-for-losses-related-to-hacking-can-continue/?_r=0*, last accessed Feb. 3, 2015. "Another Target data-breach lawsuit can proceed, judge says," available at *http://www.startribune.com/business/286412161.html*, last accessed Feb. 3, 2015.

7. *See* "'Inception' Cyber Espionage Campaign Targets PCs, Smartphones," available at *http://www.darkreading.com/perimeter/inception-cyber-espionage-campaign-targets-pcs-smartphones/d/d-id/1318046*, last accessed Feb. 3, 2015.

8. *See* "Hackers Stealing Business Secrets to Game the Stock Market," available at *http://www.newsweek.com/hackers-stealing-business-secrets-game-stock-market-288231*, last accessed Feb. 3, 2015; "ICANN targeted by Spear Phishing attack, several systems impacted," available at *http://www.csoonline.com/article/2860737/social-engineering/icann-targeted-by-spear-phishing-attack-several-systems-impacted.html*, last accessed Feb. 3, 2015.

9. Spear phishing is a psychologically more compelling form of phishing based upon socially engineering the email to the unsuspecting employee. *See, e.g.,* "3 low-tech threats that lead to high-profile breaches," available at *http://www.csoonline.com/article/2859482/data-protection/3-low-tech-threats-that-lead-to-high-profile-breaches.html?page=2*, last accessed Feb. 3, 2015.

10. *See* "APT Mitigation: The Human Way," available at *https://www.mandiant.com/blog/apt-mitigation-the-human-way/*, last accessed Feb. 3, 2015.

11. *See* "Phish Your Own Staff: Arming Employees to Beat Modern Attacks," available at *http://www.infosecurity-magazine.com/magazine-features/phish-your-own-staff/*, last accessed Feb. 3, 2015.

12. *See* "Spear Phishing: A Bigger Concern in 2015," available at *http://www.bankinfosecurity.com/spear-phishing-bigger-concern-in-2015-a-7742*, last accessed Feb. 3, 2015.

13. *See* "New KnowBe4 Statistics Reveal Security Awareness Training Reduces Phishing Susceptibility by 75%," available at *http://www.knowbe4.com/about-us/press-releases/security-awareness-training-reduces-phishing-susceptibility-by-75/*, last accessed Feb. 3, 2015.

14. *See* Luttgens, Pepe, and Mandia, *Incident Response and Computer Forensics,* (3rd Ed. 2014), pp.263–264.

15. *See* "The Importance of a Battle-Tested Incident Response Plan," available at *https://interact.weil.com/reaction/mailings/Cybersecurity_Alert_Dec_9_2014.pdf*, last accessed Feb. 3, 2015.

16. *See* "The Importance of a Battle-Tested Cyber Incident Response Plan," available at *https://blogs.law.harvard.edu/corpgov/2014/12/19/the-importance-of-a-battle-tested-cyber-incident-response-plan/*, last accessed Feb. 3, 2015.

17. *See* "Is Your Company Ready for a Big Data Breach? The Ponemon Second Annual Study on Data Breach Preparedness," available at *http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf*, last accessed Feb. 3, 2015.

18. *See* "Target's Lack of CISO Was 'Root Cause' of Systems Breach," available at *http://blogs.wsj.com/cio/2014/09/30/targets-lack-of-ciso-was-root-cause-of-systems-breach/*, last accessed Feb. 3, 2015.

19. *See* "Eyes turn to the next Congress as Sony hack exposes cybersecurity flaws," available at *http://www.washingtonpost.com/blogs/post-politics/wp/2014/12/18/eyes-turn-to-the-next-congress-as-sony-hack-exposes-cybersecurity-flaws/*, last accessed Feb. 3, 2015.

The Boundaries for Insider Trading Prosecutions See a Resurgence: The 1980s Are Back!

By Marc D. Powers, Mark A. Kornfeld, Jonathan A. Forman, and Margaret E. Hirce

In a closely followed appeal, the US Court of Appeals for the Second Circuit on December 10, 2014, delivered an important decision in *United States v. Newman*[1] by vacating the insider-trading convictions of two former hedge fund portfolio managers, Todd Newman and Anthony Chiasson, and directing that the charges against them be dismissed with prejudice.

This decision has significant implications for criminal insider-trading prosecutions and those brought civilly by the US Securities and Exchange Commission (SEC). Fundamentally, it will make it more difficult for the government to charge alleged remote tippees (like the defendants in this case who were three or four persons removed from the corporate insiders) with violations of the federal securities laws. Indeed, the Court appeared to be critical of the government for bringing criminal insider-trading charges against Newman and Chiasson at a point when neither corporate insider had been charged criminally for insider trading and one also has not been charged administratively or civilly.

This decision is significant because in it the Second Circuit:

- Grounds its analysis in the US Supreme Court's longstanding insider-trading decisions of *Dirks v. SEC*[2] and *Chiarella v. United States*[3] from the early 1980s, which established that "insider trading liability is based on breaches of fiduciary duty";
- Clarifies the boundaries for tippee liability by holding that the government must prove beyond a reasonable doubt that a tippee has knowledge of the personal benefit to the tipper; and
- Restricts what constitutes a personal benefit in the context of insider trading by now requiring a *quid pro quo* relationship.

According to the Second Circuit, the government's criminal case against Newman and Chiasson suffered from similar flaws that contributed to its loss in the criminal insider trading prosecution of Rengan Rajaratnam,[4] as well as the SEC's losses in 11 insider-trading cases or claims over the past year. As we pointed out last month in a BNA Securities

Marc D. Powers and Mark A. Kornfeld are Partners, and Jonathan A. Forman and Margaret E. Hirce are Associates, of Baker & Hostetler LLP.

the Corporate Governance Advisor

The ***CORPORATE GOVERNANCE ADVISOR*** (ISSN 1067-6171) is published bimonthly by Wolters Kluwer at 76 Ninth Avenue, New York, NY 10011. Subscription rate, $775 for one year. POSTMASTER: Send address changes to *THE CORPORATE GOVERNANCE ADVISOR,* Wolters Kluwer, 7201 McKinney Circle, Frederick, MD 21704. Send editorial correspondence to Wolters Kluwer, 76 Ninth Avenue, New York, NY 10011. To subscribe, call 1-800-638-8437. For Customer service, call 1-800-234-1660.

Regulation & Law Report article,[5] the SEC in all these cases stretched the law or the facts beyond fairness and reason. Like the judges and juries in those cases, the Second Circuit now appears to be setting the government straight.

Background

As part of a broader criminal insider-trading investigation, the US Attorney for the Southern District of New York, Preet Bharara, brought insider-trading charges against two hedge fund portfolio managers, Todd Newman (formerly at now-defunct Diamondback Capital Management, LLC) and Anthony Chiasson (formerly at now-defunct Level Global Investors, LP). At trial, the government provided evidence that Newman and Chiasson each traded shares of Dell and NVIDIA for their funds based upon information regarding earnings announcements that were not yet public.[6] The government showed that the corporate insiders tipped a group of research analysts, who passed along the information within the group until it was ultimately provided to analysts where Newman and Chiasson worked. In turn, the defendants each traded on the information resulting in profits of $4 million and $68 million, respectively, for their funds.

At the close of the six-week trial, Newman and Chiasson moved for a judgment of acquittal, arguing that the government failed to put forth sufficient evidence to establish that the corporate insiders exchanged confidential information for a personal benefit as required by *Dirks*. As the government failed to prove receipt of a benefit, and as tippee liability is derivative of the tipper's liability, Newman and Chiasson argued that they could not be convicted. They further argued that they could not be found guilty of insider trading, as they had no knowledge of the personal benefit to the corporate insiders, and therefore "were not aware of, or participants in, the tippers' fraudulent breaches of fiduciary duties to Dell or NVIDIA."

On December 17, 2012, the jury returned a verdict finding Newman and Chiasson guilty on all ten counts of securities fraud and conspiracy to commit securities fraud in violation of Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 promulgated thereunder. Following their sentencing,[7] Newman and Chiasson appealed, challenging among other things the instructions to the jury as failing to require that Newman and Chiasson had knowledge that the corporate insider received a personal benefit in exchange for providing confidential information, and the sufficiency of the evidence relating to their knowledge of the corporate insiders' personal benefit.

Required Element of Tippee Liability: Knowledge of Personal Benefit to the Corporate Insider

On appeal, the government argued that it need not show that either defendant knew that the corporate insiders received a personal benefit to be found criminally liable. Instead, the government argued that, according to *Dirks* and certain cases decided by the Second Circuit after *Dirks*, criminal liability for insider trading only requires that the "tippee know that the tipper disclosed information in breach of a duty."

The court rejected the government's argument as being inconsistent with the Supreme Court's 1983 holding in *Dirks* and certain holdings in post-*Dirks* cases. According to the influential Second Circuit, the government was wrong because the Supreme Court in *Dirks* was "quite clear" on three points:

- "[T]he tippee's liability derives only from the tipper's breach of a fiduciary duty, not from trading on material, non-public information."
- "[T]he corporate insider has committed no breach of fiduciary duty unless he receives a personal benefit in exchange for the disclosure." and
- "[E]ven in the presence of a tipper's breach, a tippee is liable only if he knows or should have known of the breach."

The court criticized the government for "selectively parsing" *dicta* from the post-*Dirks* cases in an attempt to "revive the absolute bar on tippee trading that the Supreme Court explicitly rejected in *Dirks*."

The Court further held that:

> [T]o sustain an insider trading conviction against a tippee, the Government must prove each of the following elements beyond a reasonable doubt: (1) the corporate insider was entrusted with a fiduciary duty; (2) the corporate insider breached his fiduciary duty by (a) disclosing confidential information to a tippee (b) in exchange for a personal benefit; (3) the tippee knew of the tipper's breach, that is, he knew the information was confidential and divulged for personal benefit; and (4) the tippee still used that information to trade in a security or tip another individual for personal benefit.

The court reasoned that this holding comports with "well-settled principles of substantive criminal law" that require a finding of *mens rea* by a defendant.

Insufficient Evidence: Personal Benefit to the Corporate Insider

The court also rejected the government's evidence, even when viewed in the light most favorable to it, because the evidence "was simply too thin to warrant the inference that the corporate insiders received any personal benefit in exchange for their tips." This holding is significant because it limits an element of insider trading that many courts have viewed broadly to include personal relationships, pecuniary gains, and even "any reputational benefit that will translate into future earnings." The court emphasized this limitation, noting that holding otherwise would mean "practically anything would qualify."

Specifically, the court found that the Dell corporate insider and intermediary tippee "were not 'close' friends, but had known each other for years, having both attended business school and worked at Dell together." Notably, the intermediary tippee testified that he would have given career advice to the corporate insider without receiving any tips because he routinely did so for colleagues. Similarly, the NVIDIA corporate insider and intermediary tippee were "family friends" or "merely casual acquaintances" who had "met through church and occasionally socialized together."

As a result, the court has made clear that in order to prove a personal benefit in the context of a personal relationship, the government must show a *quid pro quo* relationship or provide "proof of a meaningfully close personal relationship that generates an exchange that is objective, consequential, and represents at least a potential gain of a pecuniary or similarly valuable nature."

Insufficient Evidence: Knowledge of Trading on Information from Corporate Insider in Violation of Insider's Duty

The Second Circuit also found that there was "absolutely no testimony or any other evidence" that Newman or Chiasson knew that they were trading on tips obtained from corporate insiders who received a personal benefit for breaching their duty, or even that they consciously avoided learning these facts. Importantly, for subsequent cases and guidance, the court noted that "Newman and Chiasson were several steps removed from the corporate insiders." In particular, Newman and Chiasson were remote tippees three and four levels removed from the alleged Dell corporate insider, respectively, and both were four levels removed from the alleged NVIDIA corporate insider. Further, the intermediary tippees "knew next to nothing about the insiders and nothing about what, if any, personal benefit had been provided to them." Given all this, the court found that "it is inconceivable that a jury could conclude, beyond a reasonable doubt, that Newman and Chiasson were aware of a

personal benefit, when [the intermediary tippees], who were more intimately involved in the insider trading scheme as part of the 'corrupt' analyst group, disavowed any such knowledge."

Impact of the Decision: Takeaways

Ultimately, the *Newman* decision is a stern rebuke of the US Attorney's recent aggressive insider-trading prosecutions, which have been based upon unreasonably expansive interpretations of insider-trading laws that are inconsistent with *Dirks* and *Chiarella*. This decision should set the boundaries for both the US Attorney and the SEC in bringing insider-trading cases going forward against truly remote tippees who have no knowledge of the corporate source or his or her benefit. It should also cause both the US Attorney and SEC to reassess their current insider-trading investigations and prosecutions given the significant financial and reputational damage individual defendants face by just being wrongly accused of insider trading.[8]

In particular, there are at least four significant takeaways from the *Newman* decision.

- ***First***, to be guilty of insider trading, you must know the information received is nonpublic. In this sense, it seems appropriate, and not a violation of the federal securities laws, to engage in a stock trade in a company when you hear information about a company from a friend or colleague who is unaffiliated with the company, and you have no reason to believe that the information came from someone at the company who is in a breach of a duty of confidentiality (or other fiduciary duty).

- ***Second***, to be guilty of insider trading, the information must be material and not the kind of information that merely fills in the gaps.[9] In this sense, it also seems appropriate, and not a violation of federal securities laws, to use public information (for example, observing parking lots of retail stores) to flesh out or confirm investment hypotheses or assumptions—indeed, that is precisely what analysts are supposed to do.

- ***Third***, while the prior two takeaways further clarify the boundaries of insider trading prosecutions, these boundaries are far from bright lines. Given this, there is no guarantee that the government will refrain from investigating, charging, and possibly obtaining an insider-trading conviction from a jury on conduct they believe to be unlawful even when it is completely legal.

- ***Fourth***, the Second Circuit's decision in no way opens up the floodgates to indiscriminate trading on possible inside information. To the contrary, it clarifies what conduct is prohibited. Moreover, significant disincentives still exist for those who might think to engage in questionable or wrongful activities apart from any prosecutions. For example, individuals (whether they be corporate insiders or other tippees) may be fired for breaching an employment agreement or fiduciary duty, sued by an employer or third party for breaching a confidentiality agreement, or face other stiff consequences for cavalier activity.

So while hedge funds, investment banks, and other money managers should sleep a little better at night knowing that they are less likely to be caught in the prosecutorial crosshairs of the US Attorney and the SEC (based on, for example, a casual conversation one of their analysts may have with a former classmate or other acquaintance), they should still take appropriate measures to protect themselves. This may even mean passing on an otherwise innocent trade when the surrounding facts and circumstances are questionable and might pique the government's curiosity. After all, despite the Second Circuit's *Newman* decision, insider trading undoubtedly will continue to be a priority for the government, which has shown an increasing interest in money managers in recent years.

Notes

1. 2014 WL 6911278 (2d Cir. Dec. 10, 2014).
2. 463 U.S. 646 (1983).
3. 445 U.S. 222 (1980).

4. *U.S. v. Rajaratnam*, 13-cr-00211 (S.D.N.Y. July 1, 2014).

5. Marc D. Powers, Jonathan A. Forman, and Margaret E. Hirce, "A Call for Better SEC Accountability Before Bringing Insider Trading Cases," *Bloomberg BNA, Securities Regulation & Law Report*, 46 SRLR 2214 (Nov. 17, 2014).

6. Tippee liability (at issue here) addresses situations in which an "insider or misappropriator in possession of material non-public information (the 'tipper') does not himself trade but discloses the information to an outsider (a 'tippee') who then trades on the basis of the information before it is publicly disclosed." "The elements of tipping liability are the same, regardless of whether the tipper's duty arises under the 'classical' or the 'misappropriation' theory."

7. On May 2, 2013, Newman received a 54-month sentence and was ordered to pay a $1 million fine and forfeit of $737,724, whereas on May 13, 2013, Chiasson received a 78-month sentence and was ordered to pay a $5 million fine and forfeit an amount not to exceed $2 million.

8. Furthermore, as we anticipated in our 2014 Mid-Year Report, this decision will impact certain pending criminal and civil insider-trading cases, including the criminal appeal by Michael Steinberg, a former portfolio manager at now defunct SAC Capital, because his jury received the same erroneous instruction given to Newman and Chiasson's jury.

9. The "mosaic theory"—wherein analysts piece "seemingly inconsequential data together with public information into a mosaic which reveals material non-public information"—has long been viewed as a defense to an insider-trading charge. *Elkind v. Liggett & Myers, Inc.*, 635 F.2d 156, 165 (2d Cir. 1980); *see also State Teachers Retirement Board v. Fluor Corp.*, 654 F.2d 843 (2d Cir. 1981).

Responding to Corporate Political Disclosure Initiatives: Guide for In-House Counsel

By Robert Kelner, Bob Lenhard, Keir Gumbs, and Zack Parks

Despite recent setbacks, efforts by activist groups to pressure companies to disclose details of their political activities are not going away. As these groups become increasingly sophisticated, 2015 looks to be their most active year to date. In fact, for the first time ever, the Center for Political Accountability plans to issue a report this year ranking the political spending disclosure practices of all 500 companies in the S&P 500 Index. This guide highlights recent developments regarding corporate political spending disclosure efforts, looks ahead to what public companies can expect in the near future, and provides strategies and tips for those grappling with disclosure issues.

Corporate Political Spending Disclosure 101

Although federal, state, and local laws and regulations already require companies to disclose information about their lobbying and political activities, activists have long maintained that those required disclosures do not go far enough. Although laws require companies and their PACs to disclose direct contributions to candidates, they do not, for example, require companies to disclose payments to trade associations and 501(c)(4) social welfare groups—even though those groups may use the funds to influence elections. Early last decade, emboldened by their role in passing the McCain-Feingold campaign finance reform law, activists began mobilizing to pressure companies to publicly disclose more information about their political activities. Although some have argued that these efforts are primarily intended to force companies to scale back their lobbying and political activities—not to promote transparency—they continue unabated. This decade, as the courts have loosened restrictions on corporate political activity, corporate political spending disclosure efforts have picked up significant steam. In the past few years, activists have focused on four vehicles to compel corporations to publicly disclose more of their political and lobbying spending: shareholder resolutions, SEC rulemaking, "voluntary" Web site disclosure, and litigation.

Shareholder Resolutions

The most prominent tool in the disclosure advocate's toolbox is the shareholder proposal. Although shareholder resolutions generally are non-binding, they still have teeth. If a company fails to take action on a shareholder resolution that received a majority of votes cast, influential proxy advisory firms like Institutional Shareholder Services will, the following year, recommend a vote against the company's directors.

In recent years, a conglomeration of groups have increasingly called for shareholders to vote on resolutions that would require companies to disclose more information about their political spending on their Web sites. Sometimes coupled with resolutions requiring enhanced disclosure of lobbying activities, political spending resolutions call for corporations to publicly disclose their internal procedures for spending funds for political purposes, the amount of these contributions, and the names of the recipients. Some even call for corporations to prohibit political spending altogether. Often led by the New York State Common Retirement Fund, shareholders bringing these proposals include other public

Robert Kelner, Bob Lenhard, and Keir Gumbs are Partners, and Zack Parks is Special Counsel of Covington & Burling LLP.

pension funds, labor unions, religious groups, and individual "corporate gadflies." These proposals have been voluminous; for the last several years, more shareholder proposals have focused on political spending than any other topic.

SEC Rulemaking

Activists behind these shareholder resolutions also have attempted to make shareholder political-spending resolutions unnecessary by pressuring the SEC to adopt a rule that requires public companies to disclose information about their political spending. In 2011, a group of academics filed a petition for rulemaking with the SEC asking the commission to develop rules related to "corporate political spending." Although the details of what disclosure would look like are not fleshed out, the petition has prompted a record number of largely cookie-cutter comments from labor unions and members of the campaign finance reform community.

The CPA-Zicklin Index

First issued in 2011, the annual CPA-Zicklin index is a report jointly issued by the Center for Political Accountability (CPA)—a nonprofit group promoting corporate political spending disclosure—and the Zicklin Center for Business Ethics Research at the Wharton School of the University of Pennsylvania. The report ranks the top 300 companies in the S&P 500 Index based on political spending scores, according to a metric created by CPA and the Zicklin Center. Companies receive up to 70 "points" for disclosing their political expenditures and spending practices on their Web sites. For example, they can receive six points for disclosing "payments to trade associations that the recipient organization may use for political purposes" and six points for disclosing similar payments to 501(c)(4) social welfare organizations. The two dozen criteria in the Index are often arbitrary and vague. Moreover, they are moving targets year to year. Companies with low scores, however, can find themselves targets of litigation, shareholder resolutions, or public criticism.

Litigation

Activists also have looked to the courts for help in forcing companies to disclose more information about their political spending. In early 2013, the New York State Common Retirement Fund sued Qualcomm in Delaware Chancery Court seeking access, as a Qualcomm shareholder, to Qualcomm's records related to political spending. The complaint cited a provision of Delaware law that, in certain narrow cases, requires companies to give shareholders access to the "books and records" of the company.

Later that year, shareholder activists at Citizens for Responsibility and Ethics in Washington (CREW) tried another tactic. They filed a lawsuit against Aetna claiming that Aetna misled shareholders when it published a proxy statement opposing a political-spending shareholder resolution. The complaint used the proxy statement's reference to prior company political contribution reports on its Web site as a hook for asserting that alleged inaccuracies in those reports derivatively resulted in a false and misleading proxy statement.

Recent Setbacks for Disclosure Activists

Despite the many tools in their toolbox, to date, the activist efforts described previously have been largely unsuccessful. The New York State Common Retirement Fund's dubious legal theory in the *Qualcomm* litigation was never tested because the lawsuit was promptly dismissed after Qualcomm agreed to disclose more information on its Web site, something it already planned to do before it was sued. (Covington represented Qualcomm in that suit.) The *Aetna* lawsuit is still working its way through the courts.

Moreover, the SEC has put the political-spending rulemaking petition on the back burner. In 2012, the SEC added the potential rule to the semiannual, federal government-wide Unified Agenda. Adding the rule to the

Unified Agenda was a first step in formally proposing a rule for public comment, but it did not obligate the SEC to act. In any case, in late 2013, the SEC dropped corporate political-spending disclosure from its list of regulatory priorities, a move suggesting that, at least in the short term, the SEC is unlikely to force public companies to disclose their political expenditures.

Despite their frequency—the number of such resolutions has more than doubled since 2010—shareholder resolutions on political activity have almost always failed. In the 2014 proxy season, none received a majority of votes cast. In fact, according to Conference Board, in 2014, overall support fell slightly (from 20.7 percent of votes cast in 2013 to 19.5 percent of votes cast in the examined 2014 period).

The most effective initiative to date has been the CPA-Zicklin Index, and even that initiative has failed to achieve one of its primary objectives: widespread disclosure of payments to trade associations and to 501(c)(4) social welfare organizations. Although the Index has prompted more companies to disclose their political spending, more than half of all companies surveyed (153) still receive no points for disclosing information about their trade association dues payments and only one-third (100) receive points for disclosing information about contributions to 501(c)(4) social welfare organizations. In fact, after the number of surveyed companies grew to 300 in 2014, the overall percentage of companies surveyed receiving points in these categories *declined* slightly from 2013.

The Increasingly Sophisticated Methods Employed By Activists

These setbacks should not, however, be seen as an excuse for in-house counsel to move on to worrying about other issues. As described below, activists have learned from their losses and are deploying increasingly sophisticated strategies to turn the tide.

Shareholder Resolutions

Today, shareholder resolutions on political spending are more frequent, are less likely to be dismissed, and, in some ways, are generating more support. More shareholder resolutions were submitted in 2014 than any other year (103, according to the most recent data) and a higher percentage proceeded to a vote (83.5 percent versus 77.2 percent in 2013). This increase can be attributed to several factors. First, the SEC generally has taken the position that such proposals cannot be excluded from company proxies unless they focus on lobbying activities specifically related to company products or services, focus on political spending and lobbying activities relating to specific areas or legislative activity, or have already been substantially implemented. Consequently companies have few legal bases upon which they can rely in order to exclude these proposals from their proxy materials. In addition, in 2013, the CPA wrote and promoted key elements of a "political disclosure and oversight resolution" for shareholders to use to pressure companies to increase their disclosure. Moreover, activist groups are becoming increasingly sophisticated at working together on these issues. In February 2014, for example, a coalition of 60 activist investors announced the submission of political-spending shareholder proposals targeted at 48 public companies.

Although overall support for political spending resolutions remains low, some warning signs suggest that trend may not last. For example, in 2014, seven proposals reached the 40 percent support level (based on a percentage of votes cast) versus only two in 2013. The influential proxy advisory firm Institutional Shareholder Services (ISS) announced in late 2013 that it will now consider whether companies provide disclosure about trade associations when evaluating how it will recommend clients vote on lobbying disclosure proposals. This was seen as an implicit endorsement of one of the key objectives of political spending disclosure activists: enhancing disclosure of corporate payments to trade associations. ISS's shifting support for trade association

disclosures might therefore result in more recommended "yes" votes on political spending and lobbying disclosure proposals.

SEC Rulemaking

While dormant for now, the petition for an SEC political-spending disclosure rulemaking continues to build momentum. In April 2014, CREW helped re-energize efforts to pressure the SEC to adopt a political spending disclosure rule by submitting its own rulemaking petition to the SEC. A well-funded grassroots campaign has generated more than a million signatures for these petitions, and the SEC continues to face pressure from Members of Congress and activists to move forward. So, although we do not expect action in the near-term from the SEC, it is difficult to predict how the rulemaking might develop after the next election.

CPA-Zicklin Index

CPA's role as the major player in the political-spending disclosure arena will continue to grow this year. We expect that it will increasingly promote its CPA-Zicklin Index with op-eds, media campaigns, and press releases. Most significantly, the scope of the Index will expand dramatically this year. In 2014, the Index surveyed the top 300 companies in the S&P 500, as opposed to the top 200 from 2013. We have learned that, in 2015, CPA plans to survey the *entire* S&P 500. Those companies in the S&P that missed the cut in 2014 will therefore be scored and ranked this year. Highly ranked companies also should keep an eye on their scores in the years to come. As companies move up the ranks and as scoring metrics in the CPA-Zicklin Index become more refined, former "poster-children" for disclosure may find themselves on CPA's "bad actor" list.

What to Do in Response to Political Spending Disclosure Pressure

Companies must respond deliberately to targeted efforts to compel them to disclose more information about their political spending. When a company receives a shareholder proposal, a request to inspect its political "books and records," or a proposed score from the CPA, the worst thing the company can do is tuck it away in a file drawer and ignore it.

Handling Shareholder Proposals

A company that has received a political-spending shareholder proposal should research whether the shareholder has submitted the proposal previously to any other company and, if so, determine how the proposal fared at that company's annual meeting of shareholders. Companies also should coordinate with the various departments that may be implicated by the proposal, including, for example, the government affairs office, the corporate secretary, the legal department, and senior management to identify what activities the company may engage in that may be implicated by the proposal.

A company that has received a political-spending shareholder proposal also should consider initiating a dialogue with the shareholder regarding the proposal. This would demonstrate that the company is focused on enhancing shareholder value and maintaining an open dialogue with shareholders. More importantly, as suggested previously, SEC interpretive positions suggest that the SEC often is unwilling to allow companies to exclude political-spending shareholder proposals from their proxy materials on substantive grounds. Consequently, a company has a limited ability to exclude a political-spending shareholder proposal from its proxy materials unless the shareholder failed to comply with the eligibility or procedural requirements for a shareholder proposal. This strategy of opening a dialogue can prove fruitful. According to one study in 2012, as of August 2012, of the 71 proposals relating to political spending that were submitted, 30 were withdrawn by proponents, and 16 were allowed to be omitted from company proxy statements by the SEC.

Increase Your CPA-Zicklin Score

Companies also can take simple steps to increase their score on the CPA-Zicklin Index,

sometimes without altering current practices. These steps can help companies be perceived by these groups as good corporate citizens, removing them from activist crosshairs.

First, there are some easy pick-up points on the CPA-Zicklin Index that companies can earn without implementing burdensome internal reporting systems or disclosing invasive details about corporate political activities. For example, companies can receive points for posting to their Web sites a list of candidates and political committees supported by the corporation, something that is already publicly available on state campaign-finance agency Web sites. They also can receive points for adopting and publishing a policy that states that political contributions must "promote the interests of the company" and must "be made without regard for the private political preferences of executives." There are many other similar examples of easy ways to pick up points.

Second, CPA's ambiguous factors leave room for judgment and negotiation. CPA typically sends companies a document with their "preliminary grading" in the summer and invites them to comment. Companies should take advantage of the invitation. The Index scorers make mistakes and we have seen many cases in which a call from counsel to the CPA can help increase a low score.

Third, companies should be aware of what others are doing to receive points. CPA has awarded full credit to companies that report only those expenditures that exceed a certain threshold or that are made by a specific department. Companies also vary significantly in the level of detail they provide about trade association dues payments (that is, reporting the total amount of the payment, reporting the percentage of the payment that is not deductible as a business expense for tax purposes, or reporting both). We have compiled a database reflecting the disclosure practices of all companies that received points for trade association and 501(c)(4) disclosures in the most recent CPA-Zicklin Index. By consulting this database, we can provide clients with the least invasive and least intrusive disclosures they can make and still receive full credit. This "lowest common denominator" approach can help companies increase their scores without adding unnecessarily burdensome compliance and information gathering systems and without providing an unnecessarily intrusive level of detail about their activities.

Trinity v. Wal-Mart: Serious Implications for the Ordinary Business Exclusion

By Keir Gumbs and Reid Hooper

A common theme in 2014 regarding shareholder proposals was that companies were inappropriately using litigation as a tool to exclude shareholder proposals from their proxy materials. As we and a handful of others have said, however, this is not always the case. Shareholders are frequently the instigators of litigation involving Rule 14a-8 matters. We had a reminder of this phenomenon in late November when the U.S. District Court for the District of Delaware granted a summary judgment motion in favor of a shareholder who was seeking a declaratory judgment that it was entitled to have a shareholder proposal included in the proxy statement of Wal-Mart Stores Inc. In the *Walmart* decision, a federal court took a position that is likely to have significant repercussions for the SEC's administration of the ordinary business exclusion under Rule 14(a)-8(i)(7).

The *Trinity v. Wal-Mart* Decision

The *Trinity v. Walmart* case involved a shareholder proposal that related to a topic that most practitioners would agree involved a fairly resolved area of law: whether a shareholder proposal relating to the sale of a particular product could be excluded as relating to ordinary business. The proposal at issue requested that the charter of Wal-Mart's Compensation, Nominating and Governance Committee be amended to add the following to the Committee's duties:

> 27. Providing oversight concerning the formulation and implementation of, and the public reporting of the formulation and implementation of, policies and standards that determine whether or not the Company [that is, Wal-Mart] should sell a product that:
>
> (1) especially endangers public safety and well-being;
>
> (2) has the substantial potential to impair the reputation of the Company; and/or
>
> (3) would reasonably be considered by many offensive to the family and community values integral to the Company's promotion of its brand.

For the record, this is not an entirely novel proposal. Over the years, there have been a number of shareholder proposals that similarly sought to have companies review their products for their consistency with one or another set of corporate or broader societal values. In fact, it was a fairly straightforward no-action request that the staff granted under the ordinary business exclusion. The staff position was based on its historical view that decisions relating to the sale of particular products or services are ordinary business matters. For example, the Commission staff has granted relief under Rule 14a-8(i)(7) to companies seeking to exclude a variety of proposals relating to the pricing, sale, advertisement, packaging, design, and content of products.[1]

Ironically, the SEC had taken this exact position with respect to another proposal relating to guns that had previously been submitted to Wal-Mart.[2]

Not long after the SEC granted Wal-Mart's no-action request, the shareholder instigated litigation in federal court, seeking to enjoin the company from conducting its annual meeting without the shareholder proposal in the

Keir Gumbs is a partner and Reid Hooper is an associate with Covington & Burling LLP in the Washington, DC office. Keir and Reid both served on the shareholder proposal taskforce in the SEC's Division of Corporation Finance.

proxy materials. Although the court granted Wal-Mart's motion to deny the injunction, the court ultimately granted a summary judgment motion made by the shareholder. In ruling for the shareholder, the court noted:

> Trinity's Proposal sought a shareholder vote on amending Wal-Mart's Committee's charter to add an obligation to "provid[e] oversight concerning the formulation and implementation of … policies and standards that determine whether or not the Company should sell a product" having certain characteristics, i.e., one that especially endangers public safety, has the substantial potential to impair Wal-Mart's reputation, or would reasonably be considered by many to be offensive to the values integral to Wal-Mart's brand. (D.I. 3-1, Exh. D) At its core, Trinity's Proposal seeks to have Wal-Mart's Board oversee the development and effectuation of a Wal-Mart policy. While such a policy, if formulated and implemented, could (and almost certainly would) shape what products are sold by Wal-Mart, the Proposal does not itself have this consequence. As Trinity acknowledges, the outcome of the Board's deliberations regarding dangerous products is beyond the scope of the Proposal. Any direct impact of adoption of Trinity's Proposal would be felt at the Board level; it would then be for the Board to determine what, if any, policy should be formulated and implemented.

The court went on to note

> The significant social policy issues on which the Proposal focuses include the social and community effects of sales of high capacity firearms at the world's largest retailer and the impact this could have on Wal-Mart's reputation, particularly if such a product sold at Wal-Mart is misused and people are injured or killed as a result. In this way, the Proposal implicates significant policy issues that are appropriate for a shareholder vote. Additionally, again consistent with the 1998 Release, the Proposal is not excludable because it does not seek to "micro-manage" Wal-Mart or "prob[e] too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." (Id.) The Proposal does not involve "intricate detail" or seek to "impose specific time-frames" or dictate a "method[] for implementing complex policies." (Id.)

Based on this conclusion, the court ruled in favor of the shareholder. Although the court acknowledged that it had previously accorded significant weight to the SEC staff's *no-action letter* determination during the preliminary injunction hearing, the court noted that the final determination of the application of the ordinary business exception is for the court alone to make.

Implications for the 2015 Proxy Season

The *Wal-Mart* decision flies in the face of a long-standing line of *no-action letters*. As was noted earlier, the staff has long taken the position that proposals relating to the sale of a particular product can be excluded as relating to ordinary business. Just this year there have been a handful of shareholder proposals that were decided on this basis, including a controversial proposal submitted to FedEx that requested a report addressing how FedEx could "better respond to reputational damage from its association with the Washington D.C. NFL franchise team name controversy," which the SEC agreed could be excluded as relating to "the manner in which FedEx advertises its products and services."[3]

Read more closely, the *Wal-Mart* decision suggests that a shareholder proposal may not be excluded as relating to ordinary business if the proposal relates to a social policy issue and asks for board or committee oversight of the issue. Although this may appear to be a reasonable position at first glance, it creates an exception to the rule that is a mile wide. Specifically, most, if not all, shareholder proposals that focus on

social policy issues ask the board to review or report on the topic. In fact, the SEC specifically considered and disavowed a similar approach in 1983.[4]

The million dollar question that looms as we enter the 2015 proxy season is how the SEC will respond to this decision. Much like the *Express Scripts*[5] case earlier this year that challenged the SEC's historical approach to Rule 14a-8(i)(3) arguments, this case calls into question the SEC's historical approach to Rule 14a-8(i)(7) arguments.

There is at least some precedent for a district court decision significantly influencing an SEC interpretative position. The SEC's current approach to Rule 14a-8(i)(5) arguments is the direct result of *Lovenheim v. Iroquois Brands, Ltd*.[6] In *Lovenheim*, a federal court ruled that a shareholder proposal requesting that a committee study the methods by which its French supplier produced pâté *de foie gras* could not be excluded from Iroquois Brands' proxy materials even though its *foie gras* sales did not contribute to the company's net income and represented less than 0.05 percent of its assets.

This position was based on the court's reading of Rule 14a-8(i)(5), which allows a company to exclude a proposal that relates to less than 5 percent of a company's operations, assets, or net earnings unless the proposal is otherwise "significantly" related to the company's business. In ruling that the shareholder proposal could not be excluded, the court took the position that exclusion from proxy materials was unavailable for a proposal that is of *any* ethical or social significance and is meaningfully related to the issuer's business.

Conclusion

As suggested previously, the *Wal-Mart* case is noteworthy for a few reasons. First, the *Wal-Mart* case demonstrates that shareholders and companies alike use courts to resolve shareholder proposal disputes. This should not be too surprising. The SEC almost invites shareholder proposal litigation in the informal procedures letter that accompanies no-action responses. That letter indicates that only a district court, and not the SEC, can adjudicate shareholder proposal disputes. Second, for the second or third time *this year*, a federal court has afforded little to no deference to SEC *no-action letters*, a potentially troubling trend.

Finally, and perhaps more importantly as we head into the 2015 proxy season, it is unclear how this decision will impact the SEC's approach to the ordinary business exclusion. If the SEC were to adopt the approach taken in the *Wal-Mart* case, it would mean that numerous proposals that would otherwise be excludable as relating to ordinary business will make their way onto corporate proxies. Although it is too late for such a position to impact the proposals that shareholders choose for the 2015 proxy season, it will undoubtedly result in an increase in the number of socially oriented proposals in 2016.

In a private meeting with various participants in the shareholder proposal process this fall, the staff of the SEC's Division of Corporation Finance indicated that they would be evaluating the impact of the *Express Scripts* case on their approach to Rule 14a-8(i)(3) arguments. With the *Wal-Mart* decision, the staff will have one more thing to think about.

Notes

1. *See e.g., General Motors Corp.* (March 20, 2001) (proposal requesting that "retail sales discounts will be made available to stockholders in the same amount afforded 'vendors'"; excludable as relating to ordinary business matters, that is, discount pricing policies); *Tootsie Roll Industries, Inc.* (Jan. 31, 2002) (proposal requesting "that Tootsie Roll 'identify and disassociate from any offensive imagery to the American Indian community' in product marketing, advertising, endorsements, sponsorships, and promotions"); *Marriott International, Inc.* (Feb. 13, 2004) (proposal requesting that "that the company issue and enforce a corporate policy against any of its hotels or resorts which it owns or manages from selling or offering to sell any sexually explicit materials through pay-per-view or in its gift shop," excludable as relating to the sale and display of a particular product and the nature, content, and presentation of programming).

2. *See Wal-Mart Stores, Inc.*, (March 9, 2001) (proposal requesting that Wal-Mart "adopt a policy which refuses to sell handguns and their accompanying ammunition in any way, and that Wal-Mart return its inventories of these products to their manufacturers," excludable as relating to ordinary business, that is, the sale of a particular product).

3. *See FedEx Corporation* (July 11, 2014).

4. *See* SEC Rel. 34-20091 (August 16, 1983) ("In the past, the staff has taken the position that proposals requesting issuers to prepare reports on specific aspects of their business or to form special committees to study a segment of their business would not be excludable under Rule 14a-8(c)(7). Because this interpretation raises form over substance and renders the provisions of paragraph (c)(7) largely a nullity, the Commission has determined to adopt the interpretative change set forth in the Proposing Release. Henceforth, the staff will consider whether the subject matter of the special report or the committee involves a matter of ordinary business; where it does, the proposal will be excludable under Rule 14a-8(c)(7).").

5. *Express Scripts Holding Co. v. Chevedden*, No. 4:13-CV-2520, 2014 WL 631538 (E.D. Mo. Feb. 18, 2014).

6. 618 F. Supp. 554 (D.D.C. 1985).

The Many Governance & Cost–Savings Benefits of Mandatory Post-Vest Holding Requirements

By Laura Wanlass and Chris Fischer

Investors are increasingly concerned with equity compensation practices at public companies. Their apprehension is evident in the level of scrutiny applied by institutional investors and proxy advisory firms when deciding whether to support management requests for new or amended share authorizations. It also is evident in the consistency with which shareholder proposals are brought forth each year, requesting that companies adopt meaningful stock retention policies for executive officers.

Despite the fact that most companies in the United States have executive stock ownership guidelines, the use of pure equity holding periods is far less prevalent. This is unfortunate, as mandatory post-vest holding requirements can provide a wide range of potential governance and accounting benefits to public company issuers, which include:

- Serving as a risk mitigating feature for executive compensation programs by working in tandem with clawback policies as an enforcement mechanism for the return of incentive awards;
- Helping to further align executive interests with those of shareholders by promoting a culture of long-term executive ownership;
- Increasing the odds of institutional investor and proxy advisory firm support for new or amended share authorization requests, plus reduced risk for shareholder proposals related to equity grant practices; and
- Delivering meaningful economic value to issuers in the form of lower financial accounting expense as a result of valuation discounts that are applied to equity compensation grants when mandatory post-vest holding requirements are specifically included in award agreements.

Laura Wanlass is an Associate Partner and Chris Fischer is a Partner of Radford, an Aon Hewitt Company.

Governance Considerations

There are two common forms of holding requirements used in the US: retention ratios and pure holding periods. Retention ratios are currently more popular, as they provide executives with more flexibility. Pure holding periods are preferred by investors and proxy advisory firms, however, and they allow companies to potentially take advantage of applicable accounting discounts.

Both types of holding periods start with an ownership requirement that is stated as a percentage of the "profit shares" resulting from a long-term incentive grant (typically ranging from 50 percent to 100 percent of all such shares). Profit shares are typically defined as

(1) the shares remaining after the payment of option exercise prices and any taxes owed at the time of exercise;

(2) vested restricted stock net of shares used to satisfy withholding requirements; and

(3) shares earned at the completion of a performance share period net of shares used to satisfy withholding requirements.

In the case of retention ratios, holding periods are enforced until an existing ownership guideline policy is met. On the other hand, pure holding periods are enforced for a stated period of time, usually one to three years, regardless of whether ownership guidelines are in place or not.

Currently, Institutional Shareholder Services (ISS) analyzes the presence of holding requirements for various purposes, including:

- QuickScore Ratings—ISS gives companies positive credit in its governance rating system for the disclosure of retention ratios or holding requirements that impact 50 percent or more of all profit shares.

- Management Proposals for New or Amended Share Authorizations—Starting with new or amended share authorization requests made in 2015, the Equity Plan Evaluation Scorecard recently adopted by ISS lists holding periods as one of several factors the firm will consider when making voting recommendations on share plans.

- Management Say-on-Pay Proposals—Pursuant to ISS' Problematic Pay Practices Policy, the firm conducts a risk assessment of executive compensation programs before deciding whether to support management Say-on-Pay proposals. ISS views the implementation of robust stock ownership guidelines and equity holding requirements as a risk mitigating practice.

- Shareholder Proposals for Stock Ownership and Equity Retention Policies—Naturally, ISS reviews a company's existing ownership guidelines and holding requirements whenever shareholders call for increased equity retention requirements. When existing policies meet ISS standards, the firm is far less likely to support a shareholder proposal.

Many large institutional investors support equity holding periods in their own proxy voting guidelines. Their internal guidelines frequently come into play for Say-on-Pay votes or management requests for new or amended share authorizations.

SEC and FASB Disclosure Requirements

Although the prevalence of mandatory post-vest holding requirements increases each year as companies strengthen the corporate governance aspects of their equity programs, an often overlooked benefit is illiquidity discounts. Yet, in our experience, disclosures related to discounts for illiquidity generally lack the rigor that one might expect under applicable accounting rules. Too often, the information provided by companies does not go far enough to provide either the "significant assumptions" or the "method" used for estimating discounts. The remainder of this article examines the Accounting Standard Codification Topic 718's (ASC 718) disclosure requirements related to illiquidity discounts, as well as our opinion on "best practices" to pursue at your organization.

Under rule ASC 718-10-55-2, the minimum disclosures required for an award of equity-based compensation are as follows:

For each year for which an income statement is presented, both of the following are required:

1. A description of the method used during the year to estimate the fair value (or calculated value) of awards under share-based payment arrangements

2. A description of the significant assumptions used during the year to estimate the fair value (or calculated value) of share-based compensation awards, including (if applicable):
   a. Expected term
   b. Expected volatility
   c. Expected dividends
   d. Risk-free rate(s)
   e. Discount for post-vesting restrictions and the method for estimating it.

Even the most basic disclosure requirements for equity-based compensation contemplate the potential for post-vest selling restrictions. As a result, ASC 718 explicitly requires the disclosure of both the methods used to estimate an illiquidity discount and all of the assumptions used in the analysis. Issuers are increasingly rigorous in their disclosure of the assumptions and methods used to value option awards and performance-based equity grants, and have similar room for growth when it comes to the illiquidity discounts created by mandatory post-vest holding requirements.

Estimating Illiquidity Discounts

Most valuation practitioners apply theoretical option pricing-based models to estimate illiquidity discounts. Multiple mathematical models are available for use, the most prominent of which are the Chaffe and Finnerty models. Both approaches consider the specific duration of the restriction period created by a mandatory post-vest holding requirement and the volatility of the underlying stock when estimating potential illiquidity discounts.

Given the fact that illiquidity discounts are almost always estimated using an option pricing model, we believe the disclosures necessary to satisfy the requirements of ASC 718-10-55-2 are analogous to the disclosure requirements related to employee stock options. The disclosure should identify the model or models used to develop the illiquidity discount, as well as the assumptions used with the model. Taking these items into account, we believe the following disclosure sample satisfies the requirements of ASC 718-10-55-2:

> *The Company periodically grants time vested restricted stock units (RSUs). The RSUs vest over a period of three years following the date of grant. The shares of Company stock underlying the RSUs will be distributed on the second anniversary of the vest date. During the period between the vest date and the distribution date the employee may not sell or otherwise dispose of the shares. The Company has applied a discount for illiquidity to the price of the Company's stock when determining the amount of compensation expense to be recorded for the RSUs. The discount for illiquidity for each RSU is estimated on the date of grant using the Chaffe model and the Finnerty model, and the assumptions noted in the following table. Based on the relative strengths of each model, a 60 percent relative weighting was applied to the discount developed with the Chaffe model and a 40 percent relative weighting was applied to the discount developed with the Finnerty model. Expected volatilities are based on implied volatilities from traded options on the Company's stock. The expected dividend yield assumptions are based on the dividend yield on the Company's stock as of the date of grant. The risk-free rates are based on the US Treasury yield curve in effect at the time of grant. The weighted-average grant-date grant illiquidity discount during the years 2014, 2013, and 2012 was 12.4 percent, 13.7 percent, and 15.1 percent, respectively. The weighted average grant date fair value of RSUs granted during 2014, 2013 and 2012 was $82.06, $64.55, and $56.53, respectively, after the application of the illiquidity discount.*

In our view, this disclosure example aligns with the intent of ASC 718-10-55-2 because it specifically calls out the size of the illiquidity discount, the models used to estimate the illiquidity discount, and the assumptions used in the analysis. Unfortunately, examples of this quality are few and far between, suggesting that issuers have ample room for improvement.

Conclusion

We anticipate that continued pressure from institutional investors and proxy advisory firms on corporate governance issues, coupled with the financial accounting benefits of illiquidity discounts will contribute to increased adoption of mandatory post-vest holding requirements over the next three to five years. As the popularity of this practice accelerates, however, so too will scrutiny from auditors and regulators. When it comes to realizing the benefits of illiquidity discounts, companies will need to be more rigorous in the valuation techniques, assumption development and disclosure practices. To that end, we counsel companies considering mandatory post-vest holding requirements to carefully review the disclosure example as a best practice model, and to review their valuation approach.

A Call for Relevant Proxy Redesign

By Elizabeth M. Dunshee and Alexis C. Hamilton

The approaching proxy season presents an opportunity to update and refresh the proxy statement to meet evolving investor needs and expectations. The trend among companies of every size is to enhance user-friendly features to transform disclosures that are merely responsive to SEC rules into proactive messages for investors. Disclosure updates may be driven by say-on-pay votes, investor activism on a particular topic or revisions by peer companies. In addition, proxy statements have become a tool to enhance shareholder engagement, improve corporate branding, advocate management's position on past performance, and introduce management's strategic vision for the future.

The key to proxy redesign is relevancy. Proxy redesign should improve the functionality of the document, highlight significant information, and generally enhance the reader's experience. It should not distract the reader or otherwise incorporate design elements that do not advance the underlying message. When used effectively, proxy redesign can reduce the length of a proxy statement, providing cost savings and improving the reader's experience. For example, *TheCorporateCounsel.net* notes that Weatherford International saw a 25 percent reduction in proxy statement length (including a 40 percent reduction in Compensation Discussion and Analysis (CD&A)) following proxy redesign efforts.

Recommended areas of focus during the proxy refreshment process are content and readability, online navigability, design, and access to complementary information.

Elizabeth M. Dunshee is a Partner, and Alexis C. Hamilton is an Associate, of Fredrikson & Byron, P.A.

Proxy Statement Content and Readability

Investors must be able to engage with the proxy materials in order to absorb a company's messaging. As proxy disclosures have expanded to comply with the SEC's complex disclosure rules and regulations, it has become increasingly important to draw investor attention to important information through the use of summaries and supplemental disclosures that are responsive to investor feedback. Below are seven tips for improving the content and readability of the proxy statement:

1. *Engage with Shareholders*: Understanding what information is relevant to investors is fundamental to improving proxy statement content. Shareholder engagement is a year-round effort, primarily coordinated between a company's investor relations and legal teams. It is no longer confined to the largest of companies. As noted in the July 2014 ProxyPulse published by Broadridge and PricewaterhouseCoopers (which summarized voting results and governance trends based on more than 4,000 annual meetings held between January 1 and June 30, 2014), mid-, small-, and micro-cap companies continue to experience weakening say-on-pay results and could benefit from increased levels of shareholder engagement. Likewise, approximately 50 percent of respondents in a May 2014 Ernst & Young (E&Y) survey of S&P 500 companies stated that they had not only engaged in conversations with shareholders, but had added disclosure to the proxy statement that was responsive to those conversations. Moreover, half of such disclosures described company changes that had resulted from the shareholder feedback.

   Shareholder feedback, as well as responsive proxy statement disclosure, frequently

relates to executive compensation. It also may cover corporate governance topics such as director tenure and diversity, executive succession planning, management of the company's opportunities and risks, and social responsibility topics such as sustainability. Companies that conduct ongoing discussions with shareholders are better able to avoid unexpected shareholder proposals and voting outcomes as well as improve investors' trust of the board and management. Careful management of the engagement process and ongoing refocusing of the dialogue can alleviate the potential risks of inconsistent messaging, competitive harm, and commitment to impractical deliverables.

2. *Highlight and Summarize Information of Interest*: CD&A summaries, which generally provide a brief overview of prior-year company performance and a high-level snapshot of executive compensation, have been prevalent for several years and were employed by 73 percent of the respondents to the 2014 E&Y survey. In response to greater investor focus on governance and other matters, companies are also starting to include a three- to five-page proxy statement summary to highlight governance practices, shareholder engagement efforts and executive pay changes made over the last year. The summary also can emphasize the company's strategic accomplishments and orient the reader as to the structure of the document.

3. *Feature Easy-to-Read FAQs*: Including a dedicated frequently asked question (FAQ) section near the beginning or end of the proxy statement is a small and relatively easy enhancement that can highlight key information and improve document navigation. FAQs can be helpful to readers in presenting both procedural information, such as the mechanics for voting shares, and substantive information, such as the rationale for the board's recommendations.

4. *Create an Eye-Catching Cover and Back Page*: Investors, particularly institutional investors, are inundated with proxy statements each year. Appealing cover graphics can make a company's information stand out, facilitate branding, and provide a more inviting introduction to the important disclosures. Redesigned cover pages typically include the company's name, logo, and institutional design, and may include artwork or graphics that distinguish the proxy statement from a complementary annual report. The proxy statement's back cover, which is often underutilized, can provide valuable real estate for promoting a successful corporate social responsibility campaign, highlighting company awards and recognitions, or thanking the shareholders for their investment in the company.

5. *Include Substantive Letters from the Chairpersons of the Board and Key Committees*: In order to acknowledge the board's accountability to shareholders, proxy statements are increasingly incorporating letters from the chairpersons of the board and key committees. These letters go beyond inviting shareholders to attend the meeting; they also introduce disclosure sections that describe company performance and committee work and anticipate and respond to investor concerns.

6. *Enhance Disclosure About Directors*: Board composition is expected to be a top priority among boards and investors in 2015. In light of an increasing investor focus on director nominees, more companies are providing supplemental information about directors and the board as a whole, including headshots, infographics of age, tenure, gender and diversity, skills matrices, and committee grids. Careful attention to this disclosure, along with complementary discussions with key shareholders, can facilitate consistent presentation and comparison from year to year and can reduce the risk that the supplemental information will be used as the basis for unexpected activism or other scrutiny.

7. *Continue to Refine the CD&A*: Although no new SEC disclosure rules are expected to

apply to executive compensation in 2015, shareholders and the SEC continue to take great interest in the topic and demand a plethora of information. A detailed or lengthy CD&A may benefit from a dedicated table of contents as well as an executive summary. In addition, maintaining a readable and easy-to-understand CD&A provides an opportunity for a company to frame its compensation message, particularly with respect to how its compensation philosophy and design enforce the correlation between pay and performance.

Infographics may aid investor review, for example, a pie chart that shows the mix of fixed compensation versus compensation tied to achievement of specific performance goals, or bar graphs that compare a company's compensation programs to those of its peers or demonstrate multi-year alignment between pay and performance. When presenting such information, it is important to carefully define relevant performance measures that can be consistently applied on a year-over-year basis. It also may be necessary to emphasize qualitative factors or alternative definitions of total compensation that the compensation committee considers when determining programs and payouts, particularly if the quantitative data or a generally applied definition of total compensation does not adequately represent the basis for the committee's decisions.

Online Navigability

The changing format in which proxy materials are accessed and viewed has been a catalyst in the movement towards proxy redesign. In a 2013 RR Donnelley survey, nearly 70 percent of investors reported viewing proxy materials online. Therefore, it has become increasingly important to enhance features of the proxy statement that improve the online viewing experience. Broc Romanek of *TheCorporateCounsel.net* recommends observing as an employee or family member navigates within your company's proxy statement to locate a specific disclosure; insights learned from the experience can improve the usability of disclosure for company investors. Generally speaking, however, the most important feature of online accessibility is a navigable table of contents with hyperlinks to relevant sections. It can also be helpful to include additional headings and sub-headings to help the reader identify placement within the document at any given point.

Design

Design elements, when used thoughtfully and consistently, can transform a dry disclosure document into a visually compelling and accessible memorandum of the company's message. The most beneficial design tools include improved use of white space; adjusted font type, size, and color; inclusion of call-out boxes with key information or director quotes; and incorporation of tables, charts, timelines or other infographics.

As noted previously, it is important to be thoughtful about proxy design. Design choices should highlight company success, but should be developed carefully to enable year-over-year consistency, and infographics should be used only when graphic representation enhances clarity for the reader. Inconsistent design and overly complex infographics can suggest that the company is attempting to cherry-pick highlights, or worse, to hide results and mislead the investor.

Access and Complementary Information

Although redesign of the proxy is central to the proxy refresh process, it is also important to consider improving shareholder access to related information. In the digital era, many companies are refreshing their investor relations Web pages, and, in particular, dedicating a separate page to annual meeting materials. Dedicated annual meeting Web pages make proxy materials and messaging easier to find and can enhance shareholder engagement with company-driven content. These materials may

include short videos from the company's CEO, chairperson, and individual directors, which tend to be more captivating than a written document, or may identify endorsements from proxy advisors. An investor relations team that works closely with legal counsel can ensure that all required SEC filings are made in connection with these postings.

How to Plan for Success

Proxy redesign affords a number of investor relations opportunities. Although the evolution of a proxy statement from a disclosure document to an investor-friendly tool may take a number of years, the first year of the refresh process is typically the most intense. Conversations about redesign ideas and processes should begin as early as possible, preferably prior to the first draft of substantive disclosures. It will be important to identify the new proxy team, which in addition to the company's transfer agent, legal counsel, proxy solicitor, and financial printer may include a company's marketing or investor relations departments or a document design and publishing firm. Planning early helps orient the team to the redesign process, align strategic thinking and insights, create a timetable and best use limited management time. A postmortem review of the process also is recommended in order to discuss lessons learned and incorporate feedback for the following year. Finally, because the proxy process is ever-evolving, companies should continue to analyze their disclosures annually to identify areas for growth and improvement.

Wolters Kluwer

Wolters Kluwer
The Corporate Governance Advisor
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

TIMELY REPORT
Please Expedite

March/April 9900529049