LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 25, Number 7 • November 2010

Medical Marijuana

Balancing Employer Drug Testing Policies with Employee Prescriptions

By Jeffrey S. Shapiro and Eric B. Martin

The issue of medical marijuana has been getting a lot of attention lately, particularly following the Obama administration's announcement last fall that it would not raid medical marijuana dispensaries if they were dispensing marijuana in accordance with state law. Since then, the number of dispensaries has exploded in the 14 states that have enacted medical marijuana laws. These states are Alaska, California, Colorado, Hawaii, Maine, Michigan, Montana, Nevada, New Jersey, New Mexico, Oregon, Rhode Island, Vermont, and Washington. Several other states are likely to enact similar laws soon. It is estimated that there are more than 300,000 medical marijuana users in the country today.

State Laws vs. Employer Policies

In the employment context, the medical marijuana discussion focuses primarily on the friction between these state laws and employers' drug policies, many of which provide "zero tolerance" for employees (or job applicants) who test positive for marijuana or other illegal drugs. The majority of employers use some form of drug testing as part of their drug policy. This may include a

continued on page 11

SEC Adopts Long-Awaited Proxy Access Rules

Agrees to Delay Effectiveness Pending Federal Court Challenge

By Robert S. Reder and George A. Esposito Jr.

Much has been written, and there will be much more to follow, about this past summer's enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Wall Street Reform Act"). By its terms, the Wall Street Reform Act is intended "[t]o promote the financial stability of the United States by improving accountability and transparency in the financial system, to end 'too big to fail,' to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes." The Wall Street Reform Act is incredibly broad in scope and dwarfs the Sarbanes-Oxley legislation that followed the accounting scandals of the previous decade.

Perhaps to the surprise of some who did not closely follow the debate, included among the provisions of this massive legislative effort are several that will impact the corporate governance and securities law disclosure requirements of U.S. public companies generally, regardless of whether they are engaged in the financial services or related industries. The full impact of these provisions will not be determinable until the Securities and Exchange Commission ("SEC") issues enabling rules. Recently, as discussed below, the SEC fulfilled one of its obligations under the Wall Street Reform Act by adopting long-awaited and much debated proxy access rules.

Background – Proxy Access Rules

In Release No. 33-9136 entitled "Facilitating Shareholder Director Nominations," which was published on Aug. 25, 2010 and is available on the SEC's Web site at http://sec.gov/rules/final/2010/33-9136.pdf (the "Release"), the SEC adopted changes to the federal proxy rules that will provide eligible shareholders with access to company proxy materials for the purpose of nominating candidates for election to the board of directors. The new rules were facilitated by passage of the Wall Street Reform Act, which includes a broad legislative mandate calling upon the SEC to adopt proxy access rules.

continued on page 2

In This Issue

Proxy Access Rules

continued from page 1

The new rules borrow heavily (with some significant changes) from controversial rules proposed but not adopted by the SEC in 2009. As with the last round of proposals, the new rules contain two key components: 1) new Rule 14a-11, providing for mandatory access to company proxy statements and cards for shareholders with a "long-term interest and commitment" in the company to nominate a limited number of director candidates; and 2) amendments to Rule 14a-8(i)(8) that narrow the "election exclusion" for shareholder proposals relating to individual director elections and terms in office.

The mammoth 451-page Release notes that proxy regulation was one of the original tasks with which the SEC was charged by Congress at the time of the adoption of the Securities Exchange Act of 1934 (the "Exchange Act"). In its earlier proposals, the SEC highlighted its concern that the federal proxy rules may not enable shareholders to exercise fully their state law rights to nominate candidates for director. The SEC considers this a "failure of the proxy process" that impedes the rights of shareholders to nominate and elect directors. Accordingly, in the SEC's view, the new rules "will benefit shareholders by improving corporate suffrage, the disclosure provided in connection with corporate proxy solicitations, and communication between shareholders in the proxy process," which in turn "will significantly enhance the confidence of shareholders who link the recent financial crisis to a lack of responsiveness of some boards to shareholder interests."

The new rules initially were scheduled to become effective on Nov. 15, 2010 and to be operative for any company whose 2011 annual shareholders meeting falls at least 120 days after that date. For any company that qualifies as a smaller reporting company (*i.e.*, those having less than $75 million in public float) under the Exchange Act, application of the new rules were deferred for three years in order to provide the SEC "with the additional opportunity," as required by the Wall Street Reform Act, "to consider whether adjustments to the rule would be appropriate for smaller reporting companies before the rule becomes applicable to them."

Commissioners' Dissent and Ensuing Litigation

Notably, however, two of the five SEC Commissioners dissented from adoption of the new rules, leading many experts to predict that litigation would ensue, even though the Wall Street Reform Act called for proxy access. It was not surprising, then, that on Sept. 29, the U.S. Chamber of Commerce and the Business Roundtable filed a lawsuit in federal court seeking to overturn the proxy access rules (citing First Amendment arguments as well as violations of states' rights) and asking the SEC to delay their effectiveness.

On Oct. 4, the SEC agreed to this delay in order to "avoid[ ] potentially unnecessary costs, regulatory uncertainty, and disruption that could occur if the new rules were to become effective during the pendency of a challenge to their validity." Accordingly, the following discussion of the new proxy access rules must be considered against the backdrop of this court challenge and the reality that, once again, proxy access is in a state of limbo.

New Rule 14a-11

New Rule 14a-11 provides holders of "a significant, long term stake in a company" with the right, under certain circumstances, to include their nominees for election as directors in the company's proxy materials in connection with annual shareholders meetings (or a special meeting held in lieu of an annual

continued on page 4

Robert S. Reder, a member of this newsletter's Board of Editors, is a New York-based partner in the Global Corporate Group of Milbank, Tweed, Hadley & McCloy LLP. **George A. Esposito Jr**. is an associate in the same group, also based in New York.

The Corporate Counselor®

EDITOR-IN-CHIEF . . . . . Adam J. Schlagman
EDITORIAL DIRECTOR . . . . . Wendy Kaplan Stavinoha
MARKETING DIRECTOR . . . . . Jeannine Kennedy
GRAPHIC DESIGNER . . . . . Louis F. Bartella

The Corporate Counselor® (ISSN 0888-5877) is published by Law Journal Newsletters, a division of ALM.

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

ALM
An Integrated Media Company

The UK Bribery Act

What U.S. Companies Need to Know

By Barry Vitou

The new UK Bribery Act comes into force in April 2011. It has been described by some as the most draconian anti-corruption law in the world. It reflects a tough new stance from UK enforcement agencies that within the last two years have ratcheted up their activity. Multi-million-dollar fines, settlements and a prison sentence have been handed out.

What It Means

While the new law is similar to the U.S. Foreign and Corrupt Practices Act ("FCPA"), companies should not be lulled into thinking that the new UK Bribery law is the same. It isn't.

The law can be summarized into four key crimes:

1. Bribing;
2. Receiving a bribe;
3. Bribing a foreign public official; and
4. Failing to prevent bribery.

Directors and officers of a company will be guilty of these offenses if they are implicated either actively or passively. I recently spoke with the general counsel to the UK's Serious Fraud Office, Vivian Robinson QC, about the new law. His view was that it brings responsibility for violations straight into the boardroom.

Failure to Prevent Bribery

The UK's Serious Fraud Office (SFO) has identified the new offense of failure to prevent bribery as one of the key weapons in its arsenal in the war against corruption. This is one of the main differences between the UK and the U.S.. The good news: There is a defense. Broadly stated, organizations that have "Adequate Procedures" to prevent bribery will not be guilty of an offense under the new law.

The UK government is currently running a guidance consultation program to educate companies on what they need to consider in the context of putting into place Adequate Procedures, but it ends on Nov. 8. This guidance is not proscriptive and companies will need to assess themselves what is appropriate.

Six Key Principles

The guidance recently published by the UK Ministry of Justice identifies six key principles that should be embodied in organizations' anti-bribery compliance programs.

1. **Risk Assessment**: Know and keep up to date with the bribery risks you face in your sector and market.
2. **Top-level Commitment**: Establish a culture across the organization in which bribery is unacceptable. If your business is small or medium-sized, this may not require much sophistication, but the purpose is to make the message clear, unambiguous and regularly repeated to all staff and business partners.
3. **Due Diligence**: Know who you do business with; this includes why, when and to whom you are releasing funds and seeking reciprocal anti-bribery agreements. Be in a position to feel confident that business relationships are transparent and ethical.
4. **Create Clear, Practical and Accessible Policies and Procedures**: Ensure that you have them and that they apply to everyone you employ, and to business partners under your effective control. Cover all relevant risks such as political and charitable contributions, gifts and hospitality, promotional expenses, and appropriate responses to demands for facilitation if an allegation of bribery comes to light.
5. **Effective Implementation**: Go beyond "paper compliance" to embed anti-bribery into your organization's internal controls, recruitment and remuneration policies, operations, communications and training on practical business issues.
6. **Monitoring and Review**. Ensure that you have audit and financial controls that are sensitive to bribery and are transparent. Consider how regularly you need to review your policies and procedures, and whether external verification would help.

The SFO's View

In addition to the six principles published by the Ministry of Justice, last year the SFO published its own list of materials on Self Reporting and what it expects to see in organizations' "Adequate Procedures." The SFO's list included the requirement for:

- Principles that are applicable regardless of local laws or culture;
- Individual accountability;
- A policy on gifts and hospitality and facilitation payments;
- A policy on outside advisers/third parties, including vetting, due diligence and appropriate risk assessments;
- A policy concerning political contributions and lobbying activities;
- Training to ensure dissemination of the anti-corruption culture to all staff at all levels within the corporation;
- A helpline within the corporation that enables employees to report concerns;
- Appropriate and consistent disciplinary processes; and
- The effect of any remedial action taken if there have been previous cases of corruption within the corporation.

continued on page 4

Barry Vitou is a partner with Winston & Strawn LLP in London, and leads the UK regulatory practice. Vitou represents clients on regulatory matters with a focus on ethics, anti-corruption and money-laundering issues. He has dealt with civil and criminal regulators in jurisdictions all over the world and has advised extensively in relation to government and criminal investigations. He is also co-author with Richard Kovalevsky QC, of www.thebriberyact.com.

UK Bribery Act

continued from page 3

Does the New Law Affect Your Business?

The UK has adopted the U.S. long-arm jurisdiction. If your company conducts business in the UK, then it is subject to the new law. In practice, any business with UK connections is at risk. It is anticipated that the meaning of "doing business" is likely to be interpreted broadly by the UK courts. The UK has followed the U.S. "global cop" approach. The new law contains no safe harbor for facilitation or "grease" payments (the payment of small sums of money to ensure someone performs his/her duty, either more promptly or at all). The legal position is therefore very clear. However, how this will work in practice is less so.

The SFO has communicated that it expects companies to adopt a zero tolerance approach to such payments, and prohibit them as part of their "Adequate Procedures." However, at the same time the SFO recognizes that stopping facilitation payments overnight is unlikely to happen and that businesses should do their best. It is hoped that the position on this area will be made clearer and we await the publication of further guidance around the prosecution of offenses under the new laws, which may throw more light on this difficult topic. At least the UK is not alone. Even with the FCPA exemption, such payments remain a thorny issue.

No Safe Harbor

Unlike the U.S. FCPA, there is no safe harbor for corporate hospitality. The SFO has said that it will be looking at examples of lavish hospitality. Corporate hospitality will need to be for an obvious and legitimate commercial purpose. What will be considered "lavish" will be a question of degree. When I interviewed Vivian Robinson, I asked him about this. He used the example of the Ryder Cup. Broadly, an organization that entertained a client at the Ryder Cup would not violate the "lavish" definition. However, if at the Ryder Cup the client was given a Rolex watch, that would be considered lavish.

Mr. Robinson emphasized that it will be critical for businesses to maintain a clear policy. The amounts spent on corporate hospitality are likely to need to be subject to upper limits. Proper books and records will also need to be kept to ensure total transparency of hospitality given and received.

What Are the Penalties?

Bluntly, if you get it wrong you risk prison. Your business risks unlimited fines, blacklisting from EU and U.S. government contracts and the forfeiture of the value of illegal deals under related money-laundering laws. Contracts obtained through a corrupt act will also be at risk of being unenforceable through illegality.

The SFO is anxious to encourage businesses to self-report and potentially avoid the harshest consequences. In light of the possible ramifications (which include serious consequences in other jurisdictions where different rules apply), a decision to report should only be made after proper investigation of the facts and specific external legal advice. This will all need to be done expediently and quickly.

The SFO adopts a carrot and stick approach to "Self Reporting." The carrot is the possibility (but no guarantee) that businesses may achieve a better outcome if they self-report. If the SFO uncovers corruption on its own (which they say is much more likely with current cooperation among authorities and better detection techniques), companies should not expect lenient treatment.

I am often asked for more generic guidance about when businesses should self-report. This will be fact-specific and is a very big step. I would not advocate that any organization self-report without having obtained independent legal advice. However, it is worth noting one aspect of the effect of the new law, which has gone largely unnoticed. That is its Trojan horse effect in respect of UK money laundering legislation.

Conclusion

The Bribery Act will require organizations to root around in the closet and conduct due diligence to engage the defense of "Adequate Procedures." If the organization suspects that a contract was obtained through a corrupt act, it could trigger a new offense under the UK's Proceeds of Crime legislation, which has even harsher sentencing penalties (14 years). There is a defense. However, broadly, it is only available if the problem is reported to the police.

As the Director of the UK's SFO, Richard Alderman, put it earlier this year: "Someone said to me … that there seems to be little downside in not coming to the SFO and in hoping that we do not find out what has happened. I could give you a number of reasons why I think that that would be wrong. Let me, though, just give you one. Which of you would like to go and visit your CEO and CFO in a police station where they are being held following arrest on money-laundering charges? Those charges will be based upon decisions by the CEO and CFO on your advice that disclosure will not be made to the SFO and that the benefit of the corruption will therefore be retained within the [corporation]. I can imagine some difficult discussions."

—❖—

Proxy Access Rules

continued from page 2

meeting). As noted in the Release, "Rule 14a-11 will apply only when applicable state law or a company's governing documents do not prohibit shareholders from nominating a candidate for election as a director." The Release notes, however, that the SEC "is not aware of any law in any state … that currently prohibits shareholders from nominating directors." Similarly, the Rule will apply to foreign private issuers that are subject to the federal proxy rules only if applicable foreign law

continued on page 8

Managing the Privacy Risks Associated with Data Outsourcing

A Practical Approach

By Elise Dieterich

The "Information Age," in which businesses collect, store, buy, sell and manage ever-increasing amounts of data, has also become the "Age of Outsourcing." When the vast amounts of personal information collected by businesses are outsourced to various types of contractors and vendors, the legal consequences can be significant. Companies can manage these risks by recognizing and addressing in their outsourcing agreements the responsibilities and potential liabilities associated with handling sensitive data. This article suggests a framework for ensuring that outsourcing agreements enhance, rather than jeopardize, data security.

Where Are the Risks?

Legislation currently pending in Congress could impose more uniform federal data privacy protections. Currently, however, unlike the European Union, Canada, and many other countries that have taken a centralized, national approach to data privacy regulation, the United States continues to take a sectoral approach, with different rules for different types and sources of personal information, and myriad inconsistent state laws. Financial information may be governed by credit reporting, banking, identity theft prevention and other financial privacy laws; health information may be governed by Department of Health and Human Services rules implementing HIPAA and HITECH; consumer information often falls under the jurisdiction of the Federal Trade Commission; and personal information derived from telephone or cable television records may be governed by Federal Communications Commission rules. In the event of a breach of personally identifiable information, such as Social Security Numbers, account numbers, dates of birth, and physical and virtual addresses, multiple state laws requiring notification to affected individuals are likely to apply. Certain types of data, such as consumer credit reports, are required by law to be destroyed when no longer in use. The list of privacy-related obligations goes on, and is growing.

A handful of states, notably Massachusetts, impose specific data protection requirements on designated information. For example, businesses that "own or license" information that includes a Massachusetts resident's first and last name in combination with a Social Security Number (SSN), driver's license or state-issued identification card number, financial account number, or credit or debit card number, are required to take "reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information" consistent with the Massachusetts rules and any applicable federal regulations. Nevada state law requires data collectors to use encryption when data storage devices containing personally identifiable information are transferred outside the secure system of a data collector, or moved beyond the data controller's "logical or physical controls." New Hampshire has enacted requirements for protection of health information that are in addition to the burdens imposed by federal law. Connecticut requires protection of SSNs in business records, and requires those who collect SSNs to post a privacy protection policy which protects the confidentiality of SSNs, prohibits the unlawful disclosure of SSNs, and limits access to SSNs.

Privacy Regulations

In general, both state and federal privacy regulations are focused on protecting individuals from exposure of information that might facilitate identity theft or other criminal acts against them, or that could reveal personal details most people prefer to keep private, including health information, financial status, e-mail communications, phone records, video rental habits, and so on. In addition, regardless of whether a specific legal obligation attaches, businesses should anticipate negative repercussions whenever information for which there is an expectation of privacy is used in a way that the employee, customer, or patient did not intend.

For these reasons, whenever a business conveys to an outside party sensitive information regarding an individual, such as the examples above, consideration should be given to how the third-party will protect such data. In the past, many businesses have assumed that a blanket assignment of liability in third-party contracts, coupled with broad hold harmless and indemnity clauses, sufficed to transfer the risk to the vendor. In the current environment of heightened data privacy concerns, however, employees, patients, and customers (and the regulators tasked to protect them) are unlikely to be satisfied by a company that simply points the finger at the vendor to which the company has elected to outsource sensitive information. This is particularly so where the company's pockets are deep and the vendor's pockets shallow, if the data loss is one that results in substantial damages or fines.

How Can Businesses Protect Sensitive Data That Is Outsourced?

The easiest way to protect sensitive data from exposure in the outsourcing process is not to outsource it at all. Consider whether the outside contractor needs to receive sensitive personal information to perform the contractor's assigned function. It is not uncommon to find that companies routinely collect and convey data points, such as SSNs or dates of birth, in contexts where that

continued on page 6

Elise Dieterich leads the Privacy & Data Security practice group at Sullivan & Worcester LLP. She can be reached at edieterich@sandw.com. This article follows on the article "Five Steps for Managing the Risks Associated with Sensitive Data," authored by Ms. Dieterich and Jonathan M. Cohen, a partner at Gilbert LLP, which appeared in the June 2010 edition of *The Corporate Counselor*.

Data Outsourcing

continued from page 5

information serves no essential purpose, but greatly increases the risk of identity theft or other potential sources of liability. Outdated employment, insurance, and medical forms, forms used to open accounts for new customers, directory forms, order fulfillment forms, and contest entry forms used to collect marketing information are common culprits. As a rule of thumb, companies should collect only what they need, and share only what they have to.

That said, there obviously are many types of sensitive information that are essential for payroll, benefits, customer service, and marketing, and that must routinely be shared with vendors in order to fulfill those functions. For information that must be outsourced, companies should start by conducting due diligence on their vendors. Ask about the vendor's internal privacy and data security policies. What administrative, physical and technological safeguards will be provided to protect the company's outsourced data? Is access to the vendor's premises controlled by key cards that track entry and exit, are file cabinets locked, and do the computer systems include up-to-date firewalls, passwords, and — if appropriate or required by law — encryption? It also is very important to ask what training the vendor provides to its employees who will handle the company's sensitive data. Are the employees versed in applicable privacy restrictions, and are there disciplinary consequences for employees who violate the rules? Does the vendor have clear policies against putting the company's sensitive information on portable storage devices, such as laptops, removable drives, etc.? Is sensitive data destroyed or returned when no longer needed?

If the vendor will further outsource any of the company's data to subcontractors, the same due diligence on those subcontractors is warranted. Indeed, proposed changes to the HIPAA rules for health care information implementing last year's HITECH Act specifically extend HIPAA obligations to both contractors and subcontractors. To state the obvious, data security is only as strong as the weakest link in the chain.

Outsourcing agreements should also explicitly address the vendor's handling of the company's information for purposes other than the primary purpose of the outsourcing agreement. For example, how is the vendor expected to respond in the event information in the vendor's possession is subpoenaed? Will the company's information be used by the vendor for the vendor's own purposes, or shared with other parties? Absent specific restrictions in the outsourcing agreement, businesses may be surprised to learn that their information has been incorporated into larger databases maintained by the vendor and/or resold to others. This occurs more commonly with demographic or customer preference information provided to third-parties for marketing purposes. Not only can such re-use of information be detrimental to the originating company's business goals, it may well violate the terms of the company's privacy policies and customer agreements, thereby potentially running afoul of Federal Trade Commission law.

Last, while assignment of liability clauses, indemnities, and hold harmless provisions may not, by themselves, adequately protect a company from legal liability and reputational damage in the event a vendor is responsible for a major data breach, these provisions should of course be included in every outsourcing agreement. In addition, the contract should address the vendor's procedures for identifying and providing notice of any data breach, and mitigating damages, should a breach occur.

What Should Be Done if a Breach Occurs?

First and foremost, if a breach of sensitive data occurs, it is imperative to act quickly to control the damage. Having a breach response plan in place before there is a problem will facilitate prompt damage control. Similarly, for outsourced information, it is essential that vendor agreements address which entity — the vendor or the company that provided the information — will be responsible for which steps in the event of a breach. Perhaps most importantly, the vendor agreement should stipulate the timeframe within which the vendor will notify the company of any breach (preferably immediately), and the steps the vendor will immediately take to plug the leak, retrieve lost information, and protect the individuals affected. In certain instances, state or federal breach notification laws will stipulate procedures that must be followed including, in some cases, notification to law enforcement. In every situation, a coordinated response by the company and its vendor will be important to minimize the company's legal liability and reputational risk.

Summary

Following are the key elements of an effective framework to protect outsourced personally identifiable information:

- Know what legal obligations attach to the information being outsourced, based on the type and source of the data the third-party vendor will receive.
- Outsource only the minimum data necessary to the task.
- Conduct due diligence on both outside contractors and their subcontractors, to verify that they have adequate data protections in place.
- Review outsourcing agreements for specific restrictions on data sharing and re-use; assignment of liability clauses, indemnities, and hold harmless provisions; and breach notification requirements.
- Have a well-thought-out breach management plan that identifies the steps both the company and its vendors will take in the event of a breach.

—❖—

Data Transfers And the EU

How Safe Is Your Policy?

By Jonathan P. Armstrong

The last couple of months have seen a number of challenges for U.S. corporations doing business in Europe, particularly those that rely on the Safe Harbor scheme to legalize the transfer of customer or employee data to the U.S. As some European regulators flex their muscles, the challenges for U.S. corporations doing business in Europe are likely to increase.

The Issue

European data protection law has a number of options for any organization wishing to export personal data from Europe to the U.S. Traditionally the most popular was through a Data Transfer Agreement (DTA), but as the form of acceptable DTA changed in Europe and the complexities of registering those DTAs with regulators in Europe increased, many corporations have turned to the Safe Harbor scheme instead.

What Is Safe Harbor?

The Safe Harbor scheme was agreed upon between the U.S. and the European Commission in 2000 as an alternative to putting DTAs in place. It allows U.S. corporations to self-certify with the U.S. Department of Commerce to standards similar to those of European privacy law. In recent years, however, Safe Harbor has encountered considerable opposition, including a report prepared by the Australian consultancy Galexia in December 2008. That report called on U.S. and European Union authorities to increase policing of the program. The main objection was that a number of organizations professing to be registered under Safe Harbor were actually not registered. Galexia said that 1,597 corporations had self-certified, but only 348 met the basic requirements of the program. While it appears that some within the U.S. Department of Commerce questioned some of Galexia's findings, the report highlighted concerns about the framework.

The German Response

At a meeting in Hannover at the end of April, a group of German privacy regulators, known as the Düsseldorfer Kreis, expressed doubts about the Safe Harbor scheme. Germany operates a regional system of data privacy regulation where each of the 16 Länder (or states) appoints its own regulator for the private sector. Those regulators try to adopt a common stance on issues affecting Germany through an informal organization, which is the Düsseldorfer Kreis. The decision says that because of the doubts over the operation of the Safe Harbor scheme, corporations can no longer take Safe Harbor self-certification as conclusive proof of adequate protection of personal data. In particular, they say that Safe Harbor certifications more than seven years old should not be treated as valid. This last point appears to warrant clarification by local regulators since, in practice, Safe Harbor requires recertification every year. In addition, Düsseldorfer Kreis called on the Federal Trade Commission ("FTC") to step up its Safe Harbor enforcement program.

Following the Düsseldorfer Kreis decision, Dr. Thilo Weichert, the data protection regulator for the German Land of Schleswig-Holstein, said on July 23, 2010 that he thinks Safe Harbor should be reviewed with a view toward the European Commission's approval of the deal with the U.S. being revoked. There is some precedent for this, as previous deals with the U.S. over air travel and bank information have been overturned. Dr. Weichert's statement made specific reference to the Galexia report, and said that Galexia was about to publish new findings that would again convey misgivings about the Safe Harbor scheme and its enforcement. He said that the FTC receives more than 2,000 complaints each year stating that corporations are not in compliance with Safe Harbor, but it has only taken enforcement action against seven corporations in the scheme's 10-year history.

What This Means for U.S. Corporations

Dr. Weichert's announcement and the earlier Düsseldorfer Kreis decision indicate that U.S. corporations will want to examine carefully any data that they hold on people in Germany. That examination will extend not only to their own operations, but also to the data handling operations of other corporations they do business with. For example, many U.S. corporations use third parties to handle data in connection with global HR systems, ethics policies, Sarbanes-Oxley whistleblower helplines, customer relationship management programs, social media operations and sales reporting systems. All of those operations are likely to contain personal data — and the system for collecting and transferring that data will need to comply with local law.

While the law in Europe is granular and each of the 27 EU member states will form its own conclusions on the adequacy of Safe Harbor, the problem is likely to spread beyond Germany. Given that the penalties for breach of data protection legislation are also on the increase across Europe, this is an area that deserves attention.

—❖—

Jonathan P. Armstrong (jparmstrong@duanemorris.com) is partner in the London office of Duane Morris LLP. A member of this newsletter's Board of Editors, Armstrong practices in the area of corporate law with a concentration in technology and compliance, counseling multinational companies on matters involving risk, technology and compliance across Europe. The author gratefully acknowledges the assistance of his colleague **Eberhard Rohm** in the preparation of this article.

Proxy Access Rules

continued from page 4

does not prohibit shareholders from making nominations. On the other hand, companies will not be permitted to opt out of the requirements of the Rule or adopt more restrictive access rules.

Notably, the new Rule is not available to shareholders who seek to change control of a board or gain more than a limited number of seats. Rather, in those instances, the procedures currently available under Rule 14a-12(c) for waging a proxy contest continue to apply.

Requirements Applicable to Nominating Shareholders

Eligibility Requirements

Minimum Beneficial Ownership Threshold:

- Three percent of the voting power of company's shares.
- Shares loaned to a third party may be included only if the shareholder has the right to recall the loaned shares and will recall the loaned shares upon being notified that any of its nominees will be included in the company's proxy materials.
- Shares sold short and borrowed shares may not be included.

Aggregation:

- To meet eligibility requirements, shareholders are entitled to aggregate their holdings.

Duration of Ownership:

- Continuous ownership (if applicable, by each group member) of the requisite amount of shares for at least three years.
- Demonstrated intent to continue to own such shares until the applicable shareholders meeting.
- Shareholders must provide disclosure concerning their intent with regard to continued ownership of the shares after the applicable shareholders meeting.

Loss of Eligibility

- If the nominating shareholder or any nominating group member submits any other nomination or participates in another group.
- If the nominating shareholder or any nominating group member separately conducts a solicitation in connection with the subject election or acts as a participant in another's solicitation.

Notice Requirements

New Schedule 14N:

- Provide notice to the company and the SEC on Schedule 14N of intent to require inclusion of nominee(s) in proxy materials (and promptly amend for any material change). Also, a final amendment would be required, within 10 days following announcement of the election results, disclosing the intention of the nominating shareholder or group with respect to continued ownership of their shares.

Deadline for Notice:

- No earlier than 150 calendar days, and no later than 120 calendar days (or if such date is a Saturday, Sunday or holiday, the next business day), prior to the anniversary of the mailing of the prior year's proxy statement.
- The deadline for submitting nominees in connection with next year's annual meeting must be included in the prior year's proxy statement.
- If a company did not hold an annual meeting during the prior year, or if the date of the meeting has changed by more than 30 calendar days from the date of the prior year's meeting, the company is required to file a Form 8-K disclosing the date by which the notice must be submitted, which date shall be "a reasonable time before the registrant mails its proxy materials for the meeting."
- Pursuant to new Item 5.08, the Form 8-K would be due "within four business days after the registrant determines the anticipated meeting date."

Schedule 14N Disclosures:

- Name and address of the nominating shareholder or each member of the nominating shareholder group, as applicable.
- Amount of shares held by each reporting person who is entitled to be voted upon in the election of directors.
- The minimum share ownership and duration of share ownership requirements are satisfied.
- To the knowledge of the nominating shareholder or group, nominee(s) satisfies the company's director qualifications, if any, as provided in company's governing documents.
- Statement from the nominee(s) consenting to being named in the proxy statement and to serving on the board if elected.
- Statement: 1) that nominating shareholder(s) intend to continue to own requisite shares through the date of the applicable shareholders meeting; and 2) regarding nominating shareholder(s) intent with respect to continued ownership after the election.
- Certification that, to the knowledge of nominating shareholder(s), shares are not held for purpose or with effect of: 1) changing control of company; or 2) gaining a number of seats on the board of directors that exceeds the maximum number of nominees that the company is required to include.
- Various disclosures about the nominating shareholder(s) and the nominee(s) consistent with disclosures currently required under the proxy rules in a contested election.
- Disclosure about the nature and extent of the relationships between the nominating shareholder or group, the nominee(s) and/or company or any affiliate of the company.
- Disclosure regarding whether the nominating shareholder

continued on page 9

Proxy Access Rules

continued from page 8

or any group member has been involved in any legal proceedings during the past 10 years.
- Disclosure of any Web site address to be used by the nominating shareholder(s) for publication of soliciting materials in support of their nominee(s).
- If desired, a statement in support of the nominee(s), not to exceed 500 words counted as currently provided in Rule 14a-8 for other shareholder proposals.

Requirements Applicable to Nominees

Independence Requirements

- Nominees must satisfy "objective" independence requirements of the national securities exchange (if any) on which company's shares are traded. Any rule requiring a "subjective determination," and more rigorous standards applicable to audit committee members or imposed in a company's governing documents or otherwise, do not have to be satisfied.

Company Exclusion of Shareholder Nominees

- The company will not be required to include a shareholder nominee if:

1. The nominee's candidacy or, if elected, board membership would violate controlling state or foreign law, the rules of a national securities exchange (other than its subjective independence requirements) or the company's governing documents.
2. The nominating shareholder or group does not satisfy the eligibility requirements of Rule 14a-11.
3. Including the nominee(s) would result in the company exceeding the maximum number of nominees it is required to include under Rule 14a 11.

- Any information required in the Schedule 14N notice either is omitted or is false or misleading in any material respect, including information as to whether the nominee satisfies the applicable "objective" securities exchange independence requirements.

Requirements Applicable to Companies

Subject Companies

- All companies subject to the SEC's proxy rules (except debt-only issuers), including voluntary filers.

Number of Nominees

- The company will not be required to include more than one shareholder nominee, or a number of nominees representing up to 25% of the board, whichever is greater.
- The maximum number includes any nominees that the company voluntarily agrees to include on its slate after being named on a filing on Schedule 14N.
- In calculating this maximum amount, any shareholder-nominated director elected at a previous meeting whose term extends beyond the meeting in question would be counted (*i.e.*, a staggered board).
- If 25% of the board is not a whole number, the maximum number of shareholder nominees will be the closest whole number below 25%.
- If the company's board is staggered, the 25% calculation is based on the total number of board seats.

Multiple Nominating Shareholders

- In the event there are multiple eligible nominating shareholders, the nominating shareholder or group representing the highest percentage of company's voting power would have its nominees included in company's proxy materials. (This replaces the proposed "first-in" method, which would have required the company to include those nominees of the first nominating shareholder or group to give timely notice.)

Company Voting Guidelines and Recommendations

- The company will be permitted, on its proxy card, to identify any shareholder nominees as such and to include a recommendation as to how shareholders should vote (for, against or withhold).
- However, when a shareholder nominee is included on its proxy card, the company will no longer be permitted to provide shareholders with the option of voting for all company nominees as a group; rather, each company and shareholder nominee will be voted on separately.

Notification Requirements

- The company must notify nominating shareholder(s) within 14 calendar days of any objections, who in turn will have 14 calendar days to respond with corrections, provided that neither the composition of a shareholder group nor a nominee may be changed.
- No later than 80 calendar days before filing its definitive proxy materials, the company must notify the SEC if it determines that it may exclude any nominee and provide a supporting opinion of counsel.
- The company may seek informal no-action advice from the SEC.
- A notice of the company's decision to include any nominee must be given to nominating shareholder(s) no later than 30 calendar days before filing of definitive proxy materials.

Other Key Aspects of New Rules

No Preliminary Proxy Materials

- Rule 14a-6 is amended to provide that company will not be required to file preliminary proxy materials solely because of the inclusion of shareholder nominees pursuant to Rule 14a-11, even if opposed by company.

continued on page 10

Proxy Access Rules

continued from page 9

Exemptions for Communications and Solicitations

- For written and oral solicitations by shareholders seeking to form a nominating shareholder group, if:

1. Shares are not held for the purpose or with the effect of: a) changing control of issuer; or b) gaining a number of seats on the board of directors that exceeds the maximum number of nominees allowable.
2. All written soliciting materials sent to shareholders and, in the case of oral communications, a Schedule 14N cover page are concurrently filed with the SEC.

- The nominating shareholder does not subsequently engage in "soliciting or other nominating activities" outside the scope of Rule 14a-11 in connection with the subject election.
- For written and oral solicitations by a nominating shareholder or group in support of nominee(s) that the company has advised will be included in company's proxy materials, if:

1. The nominating shareholder or group does not seek the power to act as a proxy for another shareholder.
2. All written soliciting materials sent to shareholders are concurrently filed with the SEC.

- The nominating shareholder does not subsequently engage in "soliciting or other nominating activities" outside the scope of Rule 14a-11 in connection with the subject election.

Nominating Shareholder Liability

The nominating shareholder or group will be liable for any statement made in a Schedule 14N that is false or misleading regarding any material fact, or that omits any material facts necessary to make the statement not false or misleading, regardless of whether that information is included in the company's proxy statement. The company will not be responsible for such disclosure.

Incorporation by Reference

- Information included in the company proxy statement from Schedule 14N will not be incorporated by reference into company's other SEC filings that incorporate the proxy statement generally.

Amendment to Rule 14a-8

As amended in 2007, Rule 14a-8(i)(8) (aka, the "election exclusion") permits a company to exclude from proxy materials any shareholder proposal relating to the nomination or election of board members. The newly adopted amendment to Rule 14a-8(i)(8) reverses the 2007 amendments, thus enabling shareholders to require the inclusion in company proxy materials of proposals to amend (or to request an amendment of) the company's governing documents regarding nomination procedures or disclosures related to shareholder nominations, so long as the proposal would not place greater restrictions on proxy access than are set forth in Rule 14a-11 or: 1) disqualify a particular nominee; 2) remove a particular director mid-term, 3) question the "competence, business judgment or character" of any particular nominee or director; 4) seek to include a specific nominee in the company's proxy materials; or 5) "[o]therwise could affect the outcome of the upcoming election of directors."

It should be noted that Rule 14a-8 requires that a shareholder making a proposal for inclusion in the proxy materials must have continuously held at least $2,000 in market value, or 1%, of the company's voting shares for a period of one year prior to submitting the proposal. The amendments do not change this requirement.

Schedules 13D and 13G

The SEC has adopted a new exception to its beneficial ownership reporting rules for 5% shareholders that permits reporting on Schedule 13G — rather than the more detailed Schedule 13D — for shareholders or groups who engage in activities in connection with a nomination under new Rule 14a-11. However, this new exception does not apply to nominating shareholders or groups that submit a nomination pursuant to an applicable state law provision or a company's governing documents (as opposed to Rule 14a-11 itself).

Exchange Act Section 16

Current Section 16 principles continue to be applicable for determining whether nominating group members are 10% owners subject to Section 16 reporting and short-swing trading liability.

Conclusion

As evidenced by the number of aborted attempts on the part of the SEC to adopt proxy access rules, proxy access is certainly one of the more controversial corporate governance issues that the SEC has faced. So far, inclusion of a proxy access mandate in the Wall Street Reform Act has not made the task any easier. This has been a polarizing debate, and commentators cannot even agree on the impact of the newly adopted, but now delayed rules. Some believe that proxy access will negatively impact the functioning of boards of directors due to the potential election of "special interest" directors, while others see little impact in view of the eligibility requirements for shareholders to submit nominations.

This debate will remain an intellectual one, probably for at least another proxy season, until the federal courts rule on the current lawsuit. Some companies already had begun to plan ahead for proxy access by amending their advance notice bylaws to accommodate the new rules.

—❖—

Medical Marijuana

continued from page 1

pre-employment drug screen, suspicion-based testing, post-accident testing and/or random testing. One of the primary benefits of refusing to employ anyone who tests positive for illegal drugs, of course, is ensuring that employees are not impaired at the workplace.

So, when an employee presents his/her employer with a valid doctor's prescription for the use of marijuana (either before taking a drug test or after testing positive), employers are faced with a difficult dilemma. This is particularly true given the fact that a positive test for marijuana does not necessarily mean that the employee was impaired at work. In fact, it may be — and often has been in many of the cases decided thus far — that there is no reason to believe the employee ever came to work impaired but, rather, that he/she only used marijuana away from work and pursuant to a doctor's prescription.

Employers in these circumstances are left to decide whether to: 1) enforce its policy and terminate (or refuse to hire) an employee after a positive drug test; or 2) accommodate medical marijuana users by making an exception to their drug policy. There is no easy answer to this question, and employers making this determination should consider the specific circumstances and the particular state statute involved.

Negative Media Attention

However, much of the media attention on this issue has been unfavorable to employers. The reason for this is that there is a natural and obvious desire to permit patients to use medications prescribed by their doctors, especially when dealing with the pain and discomfort associated with a serious medical condition. Accordingly, employees who have been fired for their off-duty use of medical marijuana have found support in their claims that this is discriminatory and that their employers should be required to make an exception to their drug policies as an accommodation of their medical condition.

Despite this, most of the courts that have analyzed this issue have found that the employer was entitled to decide whether to permit an exception to its drug policy for medical marijuana users. The basis of these holdings has generally been twofold.

What the Laws Say

First, marijuana is still illegal under federal law. Title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (commonly referred to as the Controlled Substances Act) makes possession of marijuana illegal. The state statutes do not change that — and they cannot change that — because federal law trumps state law. Any doubt about this was removed in 2005, when the United States Supreme Court held that the federal government had the right to regulate marijuana as it saw fit regardless of conflicting state laws permitting its use. *See Raich v. Gonzales*, 545 U.S. 1 (2005). So while the state statutes provide protection against being prosecuted by the state for possession of marijuana, they generally do not protect employees in the employment context.

Every state law is different. For example, in Colorado, the right to use medical marijuana is enshrined in the state's constitution. Further, Colorado, like some other states, has a "Lawful Off-Duty Statute" that prohibits employers from disciplining employees for off-duty legal conduct. Similarly, the Michigan statute prohibits any business from denying "any right or privilege" to a medical marijuana user. So the analysis in these states may differ from that in other states. But the point remains that possession of marijuana is still illegal in all 50 states, and courts thus far have generally recognized the employer's right to enforce policies that prohibit this illegal conduct.

Second, holdings favorable to employers on this issue have also relied on the employer's right to take steps to maintain a safe workplace. Indeed, under the Occupational Safety and Health Act (and similar state statutes), employers are obligated to provide a workplace free from recognized hazards. This obligation could be read to include a duty to take reasonable steps to ensure that employees are not impaired at work and in a position to harm themselves or others.

For this reason, some federal laws require drug testing of employees. The prohibition of marijuana use for any purpose continues to be a mandate for federal contractors under the Drug-Free Workplace Act of 1988. Additionally, industries regulated by the Department of Defense and Nuclear Regulatory Commission have federally mandated requirements to maintain a drug-free workplace. Likewise, the Department of Transportation has regulations that specifically provide that transportation workers may not use marijuana even in states where its use is legal. As such, for employers covered by these laws, the decision is very clear — they must not employ anyone who tests positive for illegal drugs, including medical marijuana users.

Strong Incentives

Even aside from those industries and positions where a drug-free workplace is mandated, employers have strong incentives to ensure that no one is coming to work impaired. This is especially true for employees who are operating heaving machinery or saws, driving forklifts, or working in some position where the consequences could quickly turn tragic if they were impaired on the job. Even if an employee assures the employer that he/she will only

continued on page 12

Jeffrey S. Shapiro (jshapiro@mcguirewoods.com) is a partner with the Labor & Employment Department at McGuireWoods LLP. He advises clients on a wide range of employment-related issues, including wrongful discharge and employment discrimination. **Eric B. Martin** (emartin@mcguirewoods.com) is an associate with the firm. He focuses on traditional labor and employment law.

Medical Marijuana

continued from page 11

use medical marijuana away from work, the only way an employer can be certain of that is to maintain its "zero tolerance" policy and refuse to employ anyone who tests positive for illegal drugs.

That does not mean, however, that employers should blindly continue to enforce their "zero tolerance" policies in states where medical marijuana use is permitted under state law. Rather, employers need to decide whether they want to make an exception for medical marijuana users. There could be several reasons for an employer to make an exception to its policy.

First, an employer may simply not want to terminate employees who are strong performers and only use medical marijuana away from work, particularly since they are dealing with a serious medical condition. Of course, it is important for employers to be consistent in their policies. In other words, making an exception to its drug policy for one employee who uses medical marijuana and not for another may leave an employer exposed to a disparate treatment discrimination claim. But the point remains that employers may have a legitimate desire not to terminate a medical marijuana user. This is particularly true if the employee works in a position where the potential danger if he/she came to work impaired is much less than the types of positions discussed above (*i.e.*, receptionist, cashier).

Second, employers must also weigh the risk and cost of getting sued by an employee, under either the ADA or a state statute. Under the ADA, an employer may not discriminate against a "qualified individual with a disability" for obtaining treatment for that disability or for the side effects of that treatment. The ADA expressly provides that an employer may: 1) prohibit the "illegal use of drugs" by all employees at any time; and 2) require that employees not engage in the "illegal use of drugs" in the workplace. The term "illegal use of drugs" means the use of drugs, the possession of which is unlawful under the federal Controlled Substances Act. The term thus includes the use of marijuana for any purpose. For that reason, the ADA should not act as a bar to an employer's discipline of an employee who is using medical marijuana. This should not be interpreted to mean that such lawsuits would not be filed, and employers must still face the burden and expense of defending them.

Third, predicting the results of lawsuits is never an exact science, and it is far from certain that an employee who brings a claim against his/her employer, either for failing to accommodate the employee's disability or under a state statue, will not prevail. If the medical condition for which marijuana has been prescribed is a disability, an employee may be able to show that he or she is a "qualified individual with a disability" under the ADA. Thus, for an employment decision citing current marijuana use, an employee could state a viable claim if he or she could show that: 1) his or her underlying disability was a motivating factor in the employer's decision even if the employer was also motivated by the employee's "illegal use of drugs"; or 2) his or her "illegal use of drugs" was a mere pretext for discrimination on the basis of his underlying disability. In other words, an employee could contend that the failed drug test was not the real reason for the employment decision but, rather, that the employer's real motivation was the employee's disability.

For these reasons, employers who wish to continue to apply their "zero tolerance" policies for all employees, including medical marijuana users, should review their drug-testing policies and make sure they clearly provide that the prohibition on illegal drugs includes marijuana prescribed and used under state medical marijuana laws. This will help protect employers from the claims discussed above, and refute an allegation that the employer's stated reason for the employment decision (the positive drug test) was merely a pretext to mask the employer's discriminatory motive.

RECOMMENDATIONS

Employers can take several steps to minimize the risk of an employee lawsuit for negative employment actions related to the use of medical marijuana while maintaining a drug testing policy.

1. Make sure the drug testing policy clearly prohibits the use of any drugs and other controlled substances that are illegal under federal or state law.
2. When faced with an employee believed to be under the influence of a drug, document the facts that demonstrate the suspicion. It is far easier to defend a termination based on working under the influence than it is for a positive test.
3. If you are in a federally regulated industry such as transportation, make reference to that fact in your policies and in any disciplinary or other negative employment actions you take. Federal law will trump any stronger state protections.
4. If you are not in a federally regulated industry, consider whether the potential exposure is worth the benefits derived from a zero tolerance drug policy. You may be better off instituting a policy that allows for accommodation of medical marijuana users who have valid prescriptions and who will not be under the influence at work.

—❖—