



Rob McKenna
ATTORNEY GENERAL OF WASHINGTON
900 Fourth Avenue • Suite 2000 • Seattle WA 98164-1012

MEMORANDUM

DATE: March 13, 2007

TO: Rob McKenna, Attorney General
Maureen Scharber, Communications Consultant

FROM: Jonathan A. Mark, AAG, Antitrust Division; Mail-stop TB-14, (206) 389-3806

SUBJECT: **Research Notes re: Director Liability for Speech to NACD, Northwest Chapter**

1. Reason for the briefing. I have been asked to prepare research regarding criminal liability for directors of public corporations in preparation for General McKenna's speech to the National Association of Corporate Directors, Seattle-Northwest Chapter. Specifically, I have been asked to focus on the implications for directors of the Hewlett Packard ("HP") pretexting case and the stock options backdating investigations. This memo (1) discusses criminal liability for directors in general; (2) provides background information about both the HP pretexting case and issues surrounding the backdating of stock options; (3) discusses investigations and legal actions that have resulted from these cases; (4) discusses new legislation and current laws that may be violated by the conduct in these cases; and (5) offers general advice for what directors should be thinking about as a result of these cases.

2. Background and Issues

I. Background on Criminal Liability for Directors

Generally, a director is not liable for criminal offenses committed by the corporation via the acts of other officers and agents. However, directors of a corporation are criminally liable where the director has in some way participated with the corporation in the illegal act as a principal or as an aider, abettor or accessory. A director may also be liable for causing the corporation to violate the criminal law while conducting corporate business, such as by permitting or directing others to do so. Furthermore, directors of a corporation which are engaged in an unlawful business may be held criminally liable for the acts of subordinates done in the normal course of the business, regardless of whether or not the directing heads personally supervised the particular acts done or were personally present at the time and place of the commission of the acts. Significantly, where the crime charged involves guilty knowledge or criminal intent, it is essential to the criminal liability of a director of a corporation that the director actually and personally did the acts that constitute the offense, or that they were done at the direction or with the permission of the

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
Maureen Scharber
March 13, 2007
Page 2 of 15

director.

Provided that a director has personally directed, or caused another to violate the law, and the requisite elements of the criminal statute are satisfied, directors can be liable for their actions under any number of criminal laws. For example, directors, officers, and agents of corporations can, and have been charged with violations of food and drug laws, embezzlement, and larceny. Most recently, the conduct of directors has come under new forms of scrutiny as a result of the HP pretexting scandal and instances of stock options backdating.

II. Issues: Specific Instances of Criminal Liability

a. *The Hewlett Packard pretexting case*

i. Background

Perhaps the most widely-known case of a director being charged with violations of criminal law is the HP pretexting scandal.

By way of background, after confidential information discussed at HP's board meetings appeared in news publications in 2005, certain officers and certain members of the board of directors authorized the launch of two investigations, the first in 2005, and the next in 2006, to locate the source of the information leaks. Both investigations were authorized by then-Chairwoman Patricia Dunn, and the basis for the investigations was that the information leaked to the press was known only to board members. Certain officers and directors collectively comprised the "HP investigation team" in the secret investigation of the leaks to the media. In devising its plan, the HP investigation team sought the assistance of a top investigator, Ron DeLia, head of Security OutSourcing Solutions, Inc., with whom Hewlett Packard previously had worked on unrelated matters. Among other methods, DeLia allegedly encouraged the HP investigation team to use pretexting to obtain private cell phone and phone records of certain targeted individuals, including HP directors, employees, and unaffiliated newspaper reporters.¹ In documents delivered to reporters, HP has also acknowledged pretexting in other instances unrelated to the leak investigation.

Pretexting involves one person contacting a company and pretending to be someone they're not in order to obtain information about a particular customer. Generally, the pretexter pretends to be the actual customer, but may also pose as a reporter or family member to secure the information. These individuals sometimes feed the information to data brokers, who in turn sell individuals' private phone records to others. Private investigators have been using pretexting for

¹ Specifically, HP investigators used pretexting to obtain personal phone records of at least two board members (Thomas J. Perkins and George Keyworth) and nine reporters from the New York Times, the Wall Street Journal, and CNET.com, among others.

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
Maureen Scharber
March 13, 2007
Page 3 of 15

years. According to accounts from the media, corporations are “some of the most voracious consumers of data that can be obtained only via pretexting,” which suggests that pretexting may not be a rare tactic in corporate America.² The HP pretexting scandal only broke because former board member Tom Perkins pressured executives to disclose the truth in an SEC filing.

Other methods used in the HP investigations included physical surveillance and the deployment of an e-mail tracer program attached to a bogus e-mail message that had been sent to a reporter, that would have allowed the HP investigation team to trace the reporter’s IP address.

On September 12, 2006, George Keyworth, the identified source of the leaks, resigned. Dunn resigned as chairwoman on September 22, 2006. Current CEO Mark Hurd was asked to resign, but has refused to date. Hewlett-Packard's General Counsel, Ann Baskins also resigned. Senior Counsel, Kevin Hunsaker, another board member implicated in the investigation, refused to resign and was fired.

ii. Investigations and Legal Actions

The California Attorney General’s Office has taken several steps in response to the HP pretexting scandal. First, on October 4, 2006, the California Attorney General’s Office, under Attorney General Bill Lockyer, filed criminal charges against Dunn and four other individuals in California state court. The complaint alleges four felony counts: fraudulent wire communications, wrongful use of computer data, identity theft, and conspiracy to commit those three crimes. According to reports in the media, a trial date has not been set yet, but will likely be set sometime this spring.

Second, on December 7, 2006, the California Attorney General’s Office filed a complaint against HP together with a settlement in California Superior Court. According to the terms of the settlement, HP agreed to pay \$14.5 million to settle civil charges related to its investigations conduct. Of that amount, \$13.5 would go towards financing a new law enforcement fund to fight violations of privacy and intellectual-property rights, while \$650,000 would go to statutory damages, and the remaining amount would be used to reimburse the Attorney General’s Office for the cost of its investigation. HP also agreed to adopt a number of corporate governance reforms. Specifically, HP agreed to maintain employment of a chief ethics and compliance officer, expand the role of the company’s chief privacy officer to review HP’s investigation practices, expand the company’s employee and vendor codes to ensure that they address ethical standards regarding investigations, and also to retain an expert in the field of investigations to assist the company’s chief ethics officer with regard to investigations.

² Statement of Rob Douglas, a security consultant, in an article on CNET.com, *available at* http://news.com.com/Out+of+the+shadows%2C+a+pretexters+tale+-+page+2/2100-1029_3-6119674-2.html?tag=st.next.

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
Maureen Scharber
March 13, 2007
Page 4 of 15

According to reports in the media, at least one former HP employee has alleged that he was pretexted by the company. In 2005, HP filed suit against Karl Kamb, former vice president of business and development, alleging he stole company trade secrets. In January of this year, he counterclaimed against HP alleging that his phone records were improperly obtained and also alleging that he was instructed by HP management to spy on rival Dell.

There were also several federal investigations into the HP pretexting scandal. On January 10, 2007, the U.S. Attorney's Office for the Northern District of California filed federal identity theft and fraud charges against Bryan Wagner, one of the HP investigators. Two days later, Wagner plead guilty to the charges. Wagner was one of five people who had also been charged in California State court for his involvement in the HP pretexting case.³

The Securities and Exchange Commission ("SEC") also initiated an investigation and requested documents from HP after news of the scandal broke. Also, the Oversight and Investigations subcommittee of the House Committee on Energy and Commerce held hearings into the matter on September 28, 2006. A total of fourteen witnesses testified at this hearing. These hearings were widely televised and reported in the media. In addition, the Committee held a hearing on September 29, 2006 into internet data brokers and pretexting.

I have not located statistics on previous instances where a director of a public corporation was charged under criminal laws for authorizing investigations into employees of the corporation. However, the FTC has filed several lawsuits in federal district court against data brokers selling consumer telephone records without the consumer's knowledge or consent, and has also taken action against several companies that allegedly failed to implement reasonable procedures for safeguarding consumers' sensitive data.⁴ Most recently, on February 14, 2007, the FTC filed a complaint against a group of defendants who allegedly obtained confidential customer phone records. The FTC's complaint relies on a provision in the Telecommunications Act of 1996 which provides that a customer's phone records may only be disclosed "upon affirmative, written request by the customer."

iii. Laws that relate to Pretexting

State: The HP pretexting case has prompted several states to enact statutes that would directly prohibit the conduct that occurred in that case. During 2006, 15 states enacted statutes that

³ It is still uncertain what effect future federal efforts will have on the California case as California state law prevents individuals from being tried twice for the same crime.

⁴ The basis for these lawsuits is the FTC's authority under Section 5 of the FTC, which prohibits "unfair or deceptive acts or practices in or affecting commerce."

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
Maureen Scharber
March 13, 2007
Page 5 of 15

specifically prohibit purchasing or selling telephone-calling pattern records using fraud or deceit.⁵

Even without a law that specifically prohibits the purchase and/or sale of telephone records, state enforcement authorities had been somewhat successful in pursuing companies in the business of brokering calling records. For example, Missouri Attorney General Jay Nixon successfully sued one such company alleging violations of consumer protection laws, for falsely advertising to customers that it had procured cell phone calling records legitimately. In fact, the California AG's criminal case against Dunn falls under this category, as it has been brought under state identity theft and computer crime statutes.

Federal: From late 2005 into early 2006, a total of 13 bills were introduced in the House and Senate that related to pretexting. Only one of these bills, H.R. 4709 was able to gain any traction in the legislative process. H.R. 4709 was introduced by Representative Lamar Smith (R - TX) on February 8, 2006, and obtained unanimous approval by the House of Representatives on April 25, 2006. Although it languished in the Senate throughout most of the rest of the year, it gained new momentum after the HP pretexting scandal broke, and later passed the Senate by unanimous consent on December 8, 2006. It was signed into law by President Bush on January 12, 2007. The name of the act is the Telephone Records and Privacy Protection Act of 2006. In general, the Act makes it illegal for any person to knowingly and intentionally obtain, or attempt to obtain, confidential phone records by either false or fraudulent statements, or by accessing a customer's accounts via the internet without prior authorization from the customer. It also prohibits the sale or purchase of such information. A person who violates the provisions of the bill would be subject to fine, imprisonment, or both.

Several other Federal laws also make the act of pretexting illegal. For example, the Gramm-Leach Bliley Act, 15 U.S.C. § 6821 – 6827, makes pretexting to obtain bank records an illegal act punishable under federal law. Specifically, it prohibits the use of false pretenses, including fraudulent statements and impersonation, to obtain consumer's personal financial information, such as bank balances. This law also prohibits the knowing solicitation of others to engage in pretexting for customer information of a financial institution. Depending on the factual

⁵ For example, Maryland has enacted an "identity fraud" statute which makes it a crime for a person to "knowingly, willfully, and with fraudulent intent possess, obtain, or help another to possess or obtain any personal identifying information of an individual without that individual's consent." California has enacted a statute that prohibits the purchase, sale or attempted or conspired purchase or sale of "any telephone calling pattern record or list, without the written consent of the subscriber" or through fraud or deceit, and allows for penalties of up to one year's imprisonment and fines of up to \$2,500. The same week California enacted its statute, New York Governor George Pataki signed the New York Consumer Communication Records Privacy Act, which prohibits any person or entity from attempting to obtain, sell or transfer a telephone subscriber's "telephone record" without the written consent of the subscriber, except as otherwise permitted by law, and allows for civil penalties of up to \$1,000 per violation and permits the awarding of costs.

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
Maureen Scharber
March 13, 2007
Page 6 of 15

circumstances, federal wiretapping and illegal computer access statutes may also apply. Finally, as previously noted, the FTC has also relied on a provision in the Telecommunications Act of 1996 that prohibits the release of customer's phone records except "upon affirmative written request by the customer." 47 U.S.C. § 222(c)(2).

iv. What directors can do⁶

The fallout from the HP pretexting scandal does not mean that companies are no longer permitted to engage in internal investigations. However, with the expanding set of legal requirements under state and federal law, heightened scrutiny on the part of directors is required to ensure that investigations practices comply with applicable laws. Even if outside investigators are used, directors need to adequately supervise outsiders and properly manage them. Above all else, it is essential that directors ensure that employees and/or outside consultants who conduct investigations receive proper training, adhere to sound ethical and legal policies, and are subject to appropriate supervision.

The following have been identified as useful questions for directors to think about in relation to corporate policies: (1) what is the scope of the investigation; (2) who authorizes the investigation; (3) who supervises the investigation; (4) what sensitive information is being collected; (5) how is that information being collected and to whom is it being disclosed; (6) how is that information being managed and stored; (7) what documents result from the investigation and how will they be used; (8) is a written report of the investigation prepared; (9) what information does the company gather from or about its employees, executives and directors; (10) what confidentiality policies cover each of those groups; have background checks been authorized; (11) do any contractual provisions cover the information and its protection or use; (12) what privacy and data security policies are implicated by the investigation; (13) are vendors adequately supervised and have they been vetted for privacy law expertise; and (14) how do directors communicate and receive board materials?

b. *Stock Options Backdating*

i. Background

Stock options are a widely used form of employee incentive compensation in which the employee is given an option to purchase a certain number of shares in the company at a fixed price for a certain number of years.⁷ The price at which the option holder has the right to

⁶ This information in this section is taken from a Client Alert Newsletter produced by Goodwin Procter LLP, which is available at http://www.goodwinprocter.com/getfile.aspx?filepath=/Files/Publications/CA_Pretexing_10_25_06.pdf.

⁷ In financial terms, this is referred to as a call option.

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
Maureen Scharber
March 13, 2007
Page 7 of 15

purchase stock is the grant or exercise price,⁸ and it is usually set at the company's stock price on the date of the grant. If the exercise price is lower than the stock price, the option is said to be "in the money." If the exercise price is equal to the stock price, it is "at the money." Stock options became widespread in the late 1990s, particularly among technology companies, as a means of providing cash-strapped companies facing intense competition in the labor market with a method to attract and retain highly qualified and skilled employees.

Because the value of a stock option is higher if its exercise price is lower, the holder of a stock option prefers to be granted stock options when the stock price is at its lowest. Backdating allows a holder to choose a past date when the market was particularly low, which has the effect of inflating the value of the stock option. Although backdating itself is not illegal per se, it becomes illegal when directors fail to disclose the practice in financial reports and fail to properly account for backdated options according to Generally Accepted Accounting Principles and relevant tax laws. Most importantly, criminal liability depends on whether the directors were consciously trying to cover up the practice of backdating.

The most serious form of backdating is intentional backdating, whereby someone intentionally changes the date used to set an option's exercise price to one on which the stock's price was at a low. Backdating may also be inadvertent, such as when company actions and policies have the effect of causing an option to be granted with an exercise price that was lower than it should have been under applicable rules.⁹

ii. Investigations and Legal Actions

Over the past several years, dozens of publicly traded companies have come under civil and criminal investigation for backdating executive stock options. Currently, more than 170 companies are being investigated by the SEC, DOJ, or both, for possible fraudulent reporting of stock option grants to their top executives.¹⁰ Several of these investigations have resulted in SEC

⁸ A third name for this price is the "strike price."

⁹ Inadvertent backdating can result from poor documentation or misapplication of accounting standards. Here are two examples of inadvertent backdating: First, in order to bind the corporation, the board must act at a properly constituted meeting or by unanimous written consent. Under state corporation laws, written consents of the board are not deemed to be approved until the last director signs the consent. Thus, where the board purports to grant a stock option with an exercise price equal to the company's stock on a particular date, the actual price of a corporation's stock may have risen between the time the written consent approving the option grant was circulated and the date the last director signed it, which leads to an automatic in-the-money option. Second, under APB 25, which has since been replaced with SFAS 123, neither the grant date nor the measurement date of a stock option can fall before the date on which someone becomes an employee of a company. Specifying an earlier date, such as on the date on which the employee accepts an offer of employment, could cause the exercise price to be lower than it should be. These examples are taken from an Alert issued by the Council on Institutional Investors, *available at* <http://www.issproxy.com/pdf/CIIAlert2006.pdf>.

¹⁰ According to proxy-research firm Glass Lewis, as of March 9, 2007, 118 firms have disclosed that they

ATTORNEY GENERAL OF WASHINGTON

Rob McKenna
 Maureen Scharber
 March 13, 2007
 Page 8 of 15

enforcement actions, financial restatements, and executive terminations. Several criminal cases have been brought by the Department of Justice. In addition, the U.S. Attorney for the Northern District of California, Kevin V. Ryan, has created a local stock option backdating task force to investigate allegations of companies and individuals who engaged in options backdating.

The following chart¹¹ summarizes some of the more notable investigations:

Company	SEC investigation	DOJ investigation	Restated earnings
Apple Computer	Yes	Yes	Yes
Barnes & Noble	Yes	Yes	No
Caremark Rx	Yes	Yes	No
CNET Networks	Yes	Yes	Yes
Home Depot	Yes	Yes	No
McAfee	Yes	Yes	Yes
Research in Motion	Yes	No	Yes
UnitedHealth Group ¹²	Yes	Yes	Yes
XM Satellite Radio Holdings	Yes	No	No

Thus far, eleven former executives have been charged in government investigations of backdated stock options. The following chart¹³ summarizes this data:

Company/Officers	Agency	Date
Brocade • Gregory Reyes, former chairman and CEO. Criminal and civil fraud charges. Case pending. • Antonio Canova, former CFO. Civil securities fraud charges. Case pending. • Stephanie Jensen, former human resources director. Criminal and civil fraud charges. Case pending.	DOJ and SEC	July 20, 2006

are under investigation by the SEC, 57 say the Justice Department is investigating them and 236 have announced internal investigations.

¹¹ This list is taken from a USA Today article, *available at* http://www.usatoday.com/money/companies/regulation/2007-03-08-backdate-list_N.htm.

¹² Notably, Ohio Attorney General Marc Dann has publicly raised concerns with respect to the decision of the board of UnitedHealth Group to permit its recently ousted CEO, William McGuire, to allegedly backdate over \$2.3 billion in stock options. As the state's attorney for the Public Employees' Retirement System and the State Teachers' Retirement System, two of the lead plaintiffs in a derivative litigation pending in the District of Minnesota, Dann recently expressed his concern over this matter in a letter to UnitedHealth Group's special litigation committee, which has been investigating the alleged stock option backdating.

¹³ This list is taken from a USA Today article, *available at* http://www.usatoday.com/money/companies/2007-03-09-backdating-usat_N.htm?POE=MONISVA.

