Chicago-Kent Law Review

Volume 84
Issue 3 *Symposium: Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*

Article 9

June 2009

The Duty of Care and the Data Control Systems in the Wake of Sarbanes-Oxley

Michael R. Siebecker

THE DUTY OF CARE AND DATA CONTROL SYSTEMS IN THE WAKE OF SARBANES-OXLEY

MICHAEL R. SIEBECKER*

INTRODUCTION

A recent Securities and Exchange Commission (SEC) proposal raises some interesting questions that lie at the intersection of data-security, securities regulation, and legal theory. The SEC's proposal considers whether to exempt certain small public companies from Section 404 of the Sarbanes-Oxley Act of 2002 (SOX).[1] Section 404 requires public companies to provide management assessment and external auditing of a company's internal control systems over financial data.[2] Some have complained vigo-

* Associate Professor, University of Florida College of Law; B.A., Yale University; J.D., LL.M., M.Phil., Ph.D., Columbia University. I wish to thank Andrea M. Matwyshyn for thoughtful criticism and Dustin Hall for excellent research assistance on this and other projects. This short essay was based on a symposium speech given in early 2006. Despite some updated footnotes to support general claims, the essay does not incorporate legal developments since the date of the 2006 symposium.

1. Exposure Draft of Final Report of Advisory Committee on Smaller Public Companies, Release No. 33-8666, 71 Fed. Reg. 11,090 (proposed Mar. 3, 2006). For a discussion of the proposal, see Advisory Letter from James D. Cox, Brainerd Currie Professor of Law, Duke University School of Law, et al. to Christopher Cox, Chairman, Securities and Exchange Commission (Mar. 21, 2006), *available at* http://www.sec.gov/rules/other/265-23/26523-309.pdf. The SEC recently announced that it is performing a cost–benefit analysis of the proposed exemption. *See* Press Release, SEC, SEC Begins Small Business Costs and Benefits Study of Sarbanes-Oxley Act Section 404 (Feb. 1, 2008), *available at* http://www.sec.gov/news/press/2008/2008-8.htm.

2. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 404, 116 Stat. 745, 789 (codified at 15 U.S.C. § 7262 (2006)). For a general discussion of the Sarbanes-Oxley Act, see, for example, William J. Carney, *The Costs of Being Public After Sarbanes-Oxley: The Irony of "Going Private,"* 55 EMORY L.J. 141 (2006); Ginger Carroll, *Thinking Small: Adjusting Regulatory Burdens Incurred by Small Public Companies Seeking to Comply with the Sarbanes-Oxley Act*, 58 ALA. L. REV. 443 (2006); Lisa M. Fairfax, *Sarbanes-Oxley, Corporate Federalism, and the Declining Significance of Federal Reforms on State Director Independence Standards*, 31 OHIO N.U. L. REV. 381 (2005); Peter Ferola, *Internal Controls in the Aftermath of Sarbanes-Oxley: One Size Doesn't Fit All*, 48 S. TEX. L. REV. 87 (2006); Donald C. Langevoort, *The Social Construction of Sarbanes-Oxley*, 105 MICH. L. REV. 1817 (2007); Kate Litvak, *Sarbanes-Oxley and the Cross-Listing Premium*, 105 MICH. L. REV. 1857 (2007); Dana M. Muir & Cindy A. Schipani, *The Use of Efficient Market Hypothesis: Beyond Sox*, 105 MICH. L. REV. 1941 (2007); Lumen N. Mulligan, *What's Good for the Goose is not Good for the Gander: Sarbanes-Oxley-Style Nonprofit Reforms*, 105 MICH. L. REV. 1981 (2007); Manuel A. Utset, *Time-Inconsistent Management & the Sarbanes-Oxley Act*, 31 OHIO N.U. L. REV. 417 (2005); Thomas Wardell, Esq., *The Current State of Play Under the Sarbanes-Oxley Act of 2002*, 28 N.C. J. INT'L L. & COM. REG. 935 (2003); David A. Westbrook, *Telling All: The Sarbanes-Oxley Act and the Ideal of Transparency*, 2004 MICH. ST. L. REV. 441; Alyson M. Bagley, Note, *The Sarbanes-Oxley Act Leap of Faith: Why Investors Should Trust Corporate Executives and Accountants*, 37 SUFFOLK U. L. REV. 79 (2004); Ian L. Schaffer, Note, *An International Train Wreck Caused in Part by a Defective Whistle: When the*

rously that the costs of compliance, at least for small public companies, greatly outweigh any potential benefits.[3]

The basic fiduciary duty of care that directors and officers owe to a corporation, however, may require smaller companies to embrace enhanced internal control measures, despite any exemption from Section 404 granted by the SEC. Quite simply, in light of the "state of the art" regarding internal controls pursuant to Section 404 and the financial collapses that gave rise to SOX in the first place, the bar for satisfying the duty of care regarding internal control systems may have risen outside the statutory framework of SOX.

To the extent the fiduciary duty of care would independently require directors and officers to adopt enhanced internal controls over financial data, the task of defining a minimally acceptable monitoring system would ultimately fall not on legislatures or administrative agencies but instead on judges tasked with resolving shareholder suits.[4] While reliance on the flexibility of evolving common law rules may prove especially attractive in certain contexts, such as Internet regulation,[5] giving judges the primary responsibility for defining the proper scope of internal data control measures could produce more jurisprudential and practical problems than benefits. As a result, exempting certain small public companies from the certification and audit requirements under Section 404 of SOX would seem wrongheaded.

I. SOX AND THE EXEMPTION PROPOSAL

Congress adopted SOX in 2002 in the midst of the financial and ac-

Extraterritorial Application of Sox Conflicts with Foreign Laws, 75 FORDHAM L. REV. 1829 (2006).

3. *See* John C. Coffee, Jr., *Law and the Market: The Impact of Enforcement*, 156 U. PA. L. REV. 229, 241–42 (2007); Robert Prentice, *Sarbanes-Oxley: The Evidence Regarding the Impact of SOX 404*, 29 CARDOZO L. REV. 703, 729–30 (2007).

4. For a discussion of the relationship of Sarbanes-Oxley to traditional issues of corporate governance, see, for example, J. Robert Brown, Jr., *Criticizing the Critics: Sarbanes-Oxley and Quack Corporate Governance*, 90 MARQ. L. REV. 309 (2006); Regina F. Burch, *Director Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron*, 6 WYO. L. REV. 481 (2006); Robert Charles Clark, *Corporate Governance Changes in the Wake of the Sarbanes-Oxley Act: A Morality Tale for Policymakers*, 22 GA. ST. U. L. REV. 251 (2005); Nadelle Grossman, *Director Compliance with Elusive Fiduciary Duties in a Climate of Corporate Governance Reform*, 12 FORDHAM J. CORP. & FIN. L. 393 (2007); Aulana Peters, *Sarbanes-Oxley Act of 2002, Congress' Response to Corporate Scandals: Will the New Rules Guarantee "Good" Governance and Avoid Future Scandals?*, 28 NOVA L. REV. 283 (2004); Philip F.S. Berg, Note, *Unfit To Serve: Permanently Barring People from Serving as Officers and Directors of Publicly Traded Companies After the Sarbanes-Oxley Act*, 56 VAND. L. REV. 1871 (2003); Gordon S. Kaiser, Jr., Comment, *Fiduciary Responsibilities Under the Sarbanes-Oxley Design*, 55 CASE W. RES. L. REV. 627 (2005).

5. *See* Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on our Computers?*, 76 S. CAL. L. REV. 893 (2003).

counting scandals involving Enron, WorldCom and other corporate giants. On a large scale, those scandals threatened the basic integrity of the American capital markets. On a more parochial level, the corporate collapses significantly affected countless lives of individuals connected to the corporation, whether investors, employees or members of the community in which the collapse occurred.

SOX arguably represents the most significant set of regulations since the establishment of the modern securities regulation regime.[6] One of the primary goals motivating Congress was a desire to provide added safeguards that improve investor confidence in the accuracy of the financial disclosures of public companies.[7] While prior to SOX, publicly available financial information was based in large part simply on the data companies ultimately reported to auditors, SOX requires additional measures to safeguard the veracity of that underlying data and to improve the reliability of corporate disclosures.

To that end, Section 404 of SOX mandates that public companies include an "internal control report" in their annual report.[8] This control report must include an assessment and certification by management of the effectiveness of internal controls over financial reporting and an external audit and attestation of the control report.[9] Although neither SOX nor the SEC Rules prescribe exactly what internal controls a company must employ, the Rules provide a "safe harbor" from liability to the extent the controls comport with standards promulgated by "a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including broad distribution of the framework for

6. *See* Ellen P. Aprill, *What Critiques of Sarbanes-Oxley Can Teach About Regulation of Nonprofit Governance*, 76 FORDHAM L. REV. 765 (2007).

7. *See* Sarbanes-Oxley Act § 2 (noting that the Act is "an act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes").

8. *Id.* § 404. For a discussion of internal controls and auditing, see, for example, Matthew J. Barrett, *"Tax Services" as a Trojan Horse in the Auditor Independence Provisions of Sarbanes-Oxley*, 2004 MICH. ST. L. REV. 463; Erica Beecher-Monas, *Enron, Epistemology, and Accountability: Regulating in a Global Economy*, 37 IND. L. REV. 141 (2003); Peter Ferola, *Internal Controls in the Aftermath of Sarbanes-Oxley: One Size Doesn't Fit All*, 48 S. TEX. L. REV. 87 (2006); Daniel L. Goelzer, *Auditing Under Sarbanes-Oxley: An Interim Report*, 7 J. BUS. & SEC. L. 1 (2007); Donald C. Langevoort, *Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's "Duty of Care as Responsibility for Systems,"* 31 J. CORP. L. 949 (2006); Joseph A. Castelluccio III, Note, *Sarbanes-Oxley and Small Business: Section 404 and the Case for a Small Business Exemption*, 71 BROOK. L. REV. 429 (2005); Amy Grynol Gibbs, Note, *It's About Time: The Scope of Section 804 of the Sarbanes-Oxley Act of 2002*, 38 GA. L. REV. 1403 (2004); Tosha Huffman, Note, *Section 404 of the Sarbanes-Oxley Act: Where the Knee Jerk Bruises Shareholders and Lifts the External Auditor*, 43 BRANDEIS L.J. 239 (2004).

9. Sarbanes-Oxley Act § 404.

public comment."[10]

These internal control requirements in Section 404 relate to data security in at least two important ways.[11] First, a fairly recent study indicates that 99% of worldwide business data is digital or electronic rather than paper-based.[12] That digital or electronic data serves as the source information for the mandatory financial disclosures of public companies. Without effective internal information security controls, that source data can be changed, manipulated, created or deleted, perhaps without any means to detect or correct those alterations. Thus, absent adequate security controls, companies cannot ensure the accuracy of their financial disclosures.

Second, companies cannot accurately report the value of their "intellectual property" assets, such as trade secrets or copyrights, without adequate internal controls.[13] A simple example should make this clear. Consider the recipe for a signature soft drink of a publicly traded beverage company. That recipe ostensibly represents a trade secret, the value of which a company would typically report as "goodwill" on its balance sheet.[14] Of course, trade secrets are only valuable insofar as they are actually secret. If the beverage company digitally stores the soft drink recipe but does not have adequate internal controls that prevent access to the information, then nothing ensures that the recipe was actually secret when the company reported the recipe's value. If the secret recipe is not actually secret, the value of the intellectual property asset will necessarily be lower than reported in the company's financial statements.[15]

Despite the importance of internal information controls to the integrity of financial disclosures, the proposal before the SEC would exempt approximately 80% of public companies from some or all of SOX Section 404's internal control requirements.[16] While "small public companies"[17] would

10. *See* Rules and Regulations Under the Securities and Exchange Act of 1934, 17 C.F.R. § 240.13a-15(c) (2008). For an example of a qualifying safe-harbor framework, see, for example, Committee of Sponsoring Organizations of the Treadway Commission, Guidance on Monitoring Internal Control Systems, http://www.coso.org/IC.HTM (last visited Dec. 18, 2009).

11. For a general discussion of many other substantial connections between data security and Section 404 of SOX, see Bruce H. Nearon et. al., *Life After Sarbanes-Oxley: The Merger of Information Security and Accountability*, 45 JURIMETRICS 379 (2005).

12. Peter Lyman & Hal R. Varian, How Much Information?, http://www.sims.Berkeley.edu/how-much-info-2003/ (last visited Dec. 18, 2009).

13. *See* Bradford K. Newman, *Protecting Trade Secrets: Dealing with the Brave New World of Employee Mobility*, 17 DEC BUS. L. TODAY 25, 26–27 (2005).

14. *See* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 191 (2007).

15. *Id.*

16. *See* Cox et al., *supra* note 1.

17. Small public companies have a market capitalization of less than $787 million. *See* Exposure Draft of Final Report of Advisory Committee on Smaller Public Companies, Release No. 33-8666, 71

be exempt only from the external audit requirement, "microcap companies"[18] would be exempt from both the external audit as well as the management assessment and certification requirements.[19] Among other arguments to support the exemptions, proponents suggest that impact of fraud involving small and microcap companies would not have a significant effect on the overall integrity of the capital markets, the market already accounts for the greater risk associated with investing in smaller rather than larger companies, and the excessively high costs of compliance for small companies relative to larger public companies.

II. DATA SECURITY AND THE DUTY OF CARE

The project here is to examine whether a fiduciary duty of care might require officers and directors to adopt internal control systems, perhaps substantially similar to those envisioned by SOX, even if the SEC exempts the companies they serve from the ambit of the statute.

The duty of care requires that directors and officers act with "ordinary prudence" on behalf of the corporation.[20] Although the precise standard varies from jurisdiction to jurisdiction[21] and depends on statutes and common law principles, the duty of care generally involves three component duties. First, the duty to act in good faith requires that directors and officers act honestly, without conflicts of interest, and without condoning illegal activities. Second, the duty to employ a reasonable decision-making process forces directors and officers to make informed decisions based on adequate inquiries, monitoring of company policies and effective consultation with experts. Third, the duty to make reasonable decisions prohibits completely irrational decisions that result in an utter waste of corporate assets.

Appreciating the reach of the duty of care, however, requires understanding a closely related doctrine, the business judgment rule. The business judgment rule is a wide-spread common law presumption that business judgments of corporate officers and directors in fact satisfy the duty of care.[22] Overcoming the presumption presents an exceptionally difficult task for litigants. In general, plaintiffs must demonstrate a director's

Fed. Reg. 11,090, 11,091 (proposed Mar. 3, 2006).

18. Microcap companies have a market capitalization of less than $128 million. *See id.*

19. *Id.* at 11,104–05.

20. *See, e.g.*, Smith v. Van Gorkum, 488 A.2d 858, 871 (Del. 1985).

21. Notable distinctions exist among the standards in Delaware, in New York, and in those states that have adopted the Model Business Corporation Act.

22. *See Van Gorkom*, 488 A.2d at 872.

or officer's lack of good faith (typically through fraud, illegality, or a conflict of interest),[23] a lack of a rational decision-making process (usually judged by gross negligence in gathering information or monitoring the company),[24] or an utter lack of reasonableness in the business purpose for the decision (essentially amounting to waste of the corporate assets).[25] Moreover, the business judgment rule's presumption applies only to actual decisions—the rule does not shield directors or officers from inaction due to willful inattention. Once a court applies the business judgment rule, however, it becomes exceedingly difficult to void board actions or to impose liability on individual officers or directors.

So how does this assessment of the duty of care and the business judgment rule relate to information controls? Understanding the relationship between those two doctrines provides a platform for assessing the viability of potential claims that shareholders might bring against directors or officers for failing to implement adequate data control systems, even outside the context of SOX 404. Those duty-of-care claims fall roughly into four general categories. An assessment of the likelihood of success for each category follows.

First, shareholders may simply claim that an officer or director made a bad decision in implementing the information controls. The argument would be that the board's decision regarding the implementation of information controls was simply wrongheaded. Without more, the board's decision would enjoy the protection of the business judgment rule and remain wholly immune from attack.

Second, a plaintiff may claim that the decision about the information controls was so irrational and contrary to the interests of the company as to constitute a waste of corporate assets. This type of claim would best apply in cases where a corporation held significant intellectual property assets that were not adequately protected (e.g., the beverage company failing to protect its secret recipe). Like the first type of claim, a plaintiff would have very little chance of success because courts tend to look for any rational basis to support board decisions. To find in favor of a plaintiff, a court would typically have to conclude that the decision was improvident beyond

23. The plaintiff can show a lack of good faith by demonstrating that the decision was influenced by fraud, that the decision was illegal, or that the decision was influenced by a conflict of interest. *See, e.g., id.*

24. The plaintiff can show a lack of a rational decisionmaking process by proving gross negligence in the officers' or directors' corporate monitoring or information gathering. *See, e.g., id.* at 872–75.

25. The plaintiff can show a lack of a rational business purpose by showing that the decision resulted in a complete waste of corporate assets. *See, e.g., In re* Walt Disney Co. Derivative Litig., 907 A.2d 693, 748–50 (Del. Ch. 2005).

explanation or outside the realm of reason. Further, to the extent that the decision was motivated by the expense of the control measures, auditing services, or other protective practices, courts would likely defer to the officers' or directors' assessment. Perhaps only if the board decision regarding implementation of information controls was so lax as to constitute an invitation to steal the intellectual property assets of a corporation would a claim based on waste seem viable.[26]

Third, shareholders could advance a claim based on willful corporate inattention to data security. The strategy would be to avoid application of the business judgment rule presumption. As noted earlier, the business judgment rule simply doesn't afford protection where board members or officers embrace unconscious inaction. Instead, board members will get the business judgment rule's protection only if it considers thoughtfully an action, regardless of the ultimate substance of the decision made. The claim would seem tenable in a scenario where a small public or microcap company simply failed to address information controls once the requirements of SOX 404 were lifted.

From an instrumental perspective, the potential viability of a willful inattention claim would cause directors and officers to assess the problem of information controls, even if inaction were the ultimate decision. Thus, the result would perhaps be some sort of cost benefit analysis on the part of the company—a balancing of the potential costs of implementing internal controls weighed against any reduction in the risk of harm through data vulnerability. While the success of a shareholder claim for willful inattention might seem small, the very existence of the claim might cause a company to undertake at least some of the measures required under SOX 404 and the SEC Rules.

Finally, shareholders might claim that directors and officers failed to monitor compliance of corporate practices with applicable laws. Here, the plaintiff would usually have to prove gross negligence. For example, a viable claim based on the failure to monitor that amounts to gross negligence might arise if there was a failure to correct a known problem that could result in significant civil or criminal penalties.[27] But failure to im-

26. In effect, to prevail on this type of claim, a plaintiff would have to show that the controls were so irrational or contrary to the interests of the corporation that the controls did not merely let the proverbial fox into the henhouse but actually *invited* the fox into the henhouse.

27. At least one Delaware court has indicated that where criminal statutes clearly proscribe certain actions or behavior, a board of directors exposes itself to liability for failing to implement adequate compliance programs even if the board did not suspect any criminal wrongdoing at the company. *See In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996). For a discussion of Sarbanes-Oxley and criminal penalties, see, for example, David Hess, *A Business Ethics Perspective on Sarbanes-Oxley and the Organizational Sentencing Guidelines*, 105 MICH. L. REV. 1781 (2007); Ann

plement an *effective* compliance system would likely not surpass the hurdle of gross negligence; rather, the corporation would have to utterly disregard establishing a compliance system.[28]

Still, it seems entirely plausible to construct a claim against board members for failing to implement internal control measures where significant threats to data security were known. Similarly, because existing securities laws (outside SOX) require truthful financial disclosures and may impose significant penalties for non-compliance, boards may have a duty to implement at least some minimal data control measures to comport with those mandates.[29] Of course, the precise nature of the data control measures would remain insulated from liability under the business judgment rule. Nonetheless, a plaintiff could construct a plausible claim against a board decision for failing to implement internal control measures, regardless of the statutory exemption, where the board knew of mismanagement of data security.

Looking back at the four general categories of shareholder claims, then, it seems that shareholders might bring potentially successful claims against companies exempt from SOX 404 in two situations: (1) where there

Marie Tracey & Paul Fiorelli, *Nothing Concentrates the Mind Like the Prospect of a Hanging: The Criminalization of the Sarbanes-Oxley Act*, 25 N. ILL. U. L. REV. 125 (2004); Dana E. Hill, Note, *Anticipatory Obstruction of Justice: Pre-Emptive Document Destruction Under the Sarbanes-Oxley Anti-Shredding Statute, 18 U.S.C. § 1519*, 89 CORNELL L. REV. 1519 (2004). For a discussion of corporate whistleblowers and Sarbanes-Oxley, see, for example, Miriam A. Cherry, *Whistling in the Dark? Corporate Fraud, Whistleblowers, and the Implications of the Sarbanes-Oxley Act for Employment Law*, 79 WASH. L. REV. 1029 (2004); Terry M. Dworkin, *SOX And Whistleblowing*, 105 MICH. L. REV. 1757 (2007); Richard E. Moberly, *Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win*, 49 WM. & MARY L. REV. 65 (2007); Geoffrey Christopher Rapp, *Beyond Protection: Invigorating Incentives for Sarbanes-Oxley Corporate and Securities Fraud Whistleblowers*, 87 B.U. L. REV. 91 (2007); Valerie Watnick, *Whistleblower Protections Under the Sarbanes-Oxley Act: A Primer and a Critique*, 12 FORDHAM J. CORP. & FIN. L. 831 (2007).

28. In this monitoring setting, "gross negligence" obviously supplies a heightened standard regarding duty, and the leading case indicates that only an "utter failure to attempt to assure a reasonable information and reporting system exists" would give rise to liability. *Caremark*, 698 A.2d at 971. Another court imposed liability on a director who knew or should have known of management wrongdoing yet failed to take any corrective measures. *See* Francis v. United Jersey Bank, 432 A.2d 814, 826, 829 (N.J. 1981).

29. For a discussion of the relationship between Sarbanes-Oxley and traditional bodies of securities law, see, for example, Roberta S. Karmel, *The Once and Future New York Stock Exchange: The Regulation of Global Exchanges*, 1 BROOK J. CORP. FIN. & COM. L. 355 (2007); Frank B. Cross & Robert A. Prentice, *The Economic Value of Securities Regulation*, 28 CARDOZO L. REV. 333 (2006); Clyde Stoltenberg et al., *A Comparative Analysis of Post-Sarbanes-Oxley Corporate Governance Developments in the US and European Union: The Impact of Tensions Created by Extraterritorial Application of Section 404*, 53 AM. J. COMP. L. 457 (2005); Kourtney T. Cowart, Comment, *The Sarbanes-Oxley Act: How a Current Model in the Law of Unintended Consequences May Affect Securities Litigation*, 42 DUQ. L. REV. 293 (2004); Erica Gann, Comment, *Judicial Action in Retrograde: The Case for Applying Section 804 of the Sarbanes-Oxley Act to All Fraud Actions Under the Securities Laws*, 72 U. CIN. L. REV. 1043 (2004); Luke A. E. Pazicky, Note, *A New Arrow in the Quiver of Federal Securities Fraud Prosecutors: Section 807 of the Sarbanes-Oxley Act of 2002*, 81 WASH. U. L.Q. 801 (2003).

is an absence of decision making based on willful inattention and (2) where there has been an utter failure to correct known management abuses to comply with statutory obligations. While the chances of success even in those two situations might seem slim, as discussed in the next section, the basic viability of those claims creates arguably significant problems for courts that might outweigh a decision to exempt certain companies from the statutory mandates provided under SOX.

III. DATA SECURITY AND THE COMMON LAW

Most companies comply with the current safe harbor provided by the Rules under SOX Section 404, and as a result there is a fairly uniform adherence to the internal control standards that agency and independent experts developed. If the SEC accepts the proposed exemption, the duty of care nonetheless imposes some sort of obligations on corporations regarding information control. However, articulating the content of those obligations will be left to the courts as shareholder derivative suits arise. Necessarily, the judge-made law will rely on the duty of care and the business judgment rule to determine the requisite internal controls.

Relying on courts to determine the appropriate internal controls, via application of the duty of care and the business judgment rule, raises a variety of practical and theoretical problems for courts. Because the duty of care and the business judgment rule are vague, they do not give corporations adequate guidance for organizing their behavior. With the content of the duty and the standards for application varying from one jurisdiction to the next, a lack of uniformity would inevitably arise.[30] With respect to incentives for litigation, relying on judge-made law would encourage shareholder litigation. In contrast to the statutory framework that more precisely sets the duties, rights and obligations of various corporate actors, the very malleability of a common law regime would increase the pool of colorable claims. Moreover, to the extent a common law framework would increase the likelihood of shareholder claims, director and officer liability premiums would likely increase. Those payments, which result simply from added uncertainty under a common law regime, arguably waste corporate assets that could be dedicated more efficiently to other endeavors. Furthermore, a common law regime for assessing the propriety of internal control measures would fundamentally hamper corporate risk taking. Risk taking is

30. For example, corporations organized under California law will have different information security standards applied to them than corporations organized under Delaware law. The effect I am concerned about here is the effect on the market—non-uniform standards would raise the transaction costs of doing business.

necessary to business success, but uncertain and unpredictable standards could enhance the risk profile of corporate decisions. As a result, boards might not be willing to undertake measures with those enhanced risks, even though those same actions would have been taken under a more precisely defined statutory framework.

On a fundamental level, a significant concern about embracing a common law framework for assessing the adequacy of information controls relates the basic purposes of the business judgment rule presumption. Judges are not experts in business. From an institutional standpoint, judges seem rather ill suited to make decisions about proper business conduct. Tasking them with the primary responsibility of articulating internal information control standards represents an odd approach, at best. Courts seem to be one of the last places where sound business principles should be crafted from scratch.

Finally, the duty of care typically ignores corporate *stake*holders that a statutory framework could consider. The duty of care currently considers the corporation's interests (and arguably the *share*holders' interests) on a parochial level. The duty does not account for the effect of any particular action on stakeholders, including the employees of the company and the community the corporation inhabits. Nor does the duty account for the larger effects on market integrity, investment security, the environment, or any other aggregate issues. Thus, while the duty of care treats corporations as atomized entities that are quite divorced from these other interests, statutory frameworks articulated by legislatures or regulatory agencies could realistically and effectively take these other interests into account.

IV. CONCLUSION

Granting exemptions from legislative and regulatory frameworks should be done cautiously. In the case of the proposed exemptions from SOX's internal control measures, the SEC should reject the proposal because significant unjustifiable jurisprudential and practical problems will result.