Outline of Internal Controls Issues for General Counsel

1. **Cybersecurity**
   a. Disclosure Issues
      i. SEC CF Disclosure Guidance: Topic No. 2: *Cybersecurity* (October 13, 2011)[1]
      The SEC highlighted particular areas of disclosure in Form 10-K that may trigger cybersecurity risk or cyber incident disclosure depending on the facts and circumstances.
         1. *Risk Factors* – Disclose the risk of cyber incidents (Item 503(c) of Reg. S-K[2])
         2. *MD&A* – Address cybersecurity risks and cyber incidents if the costs of other consequences associated with one more or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect (Item 303(a)(3)(ii) of Reg. S-K)
         3. *Business* – Disclose to the extent a cyber incident materially affects the company's products, services, relationships with customers or suppliers, or competitive conditions (Item 101 of Reg. S-K)
         4. *Legal Proceedings* – Disclose a material pending legal proceeding that involves a cyber incident (Item 103 of Reg. S-K)
         5. *Financial Statements* – A number of situations involving cybersecurity risks and cyber incidents could impact financial statement disclosures
         6. *Disclosure Controls and Procedures* – Disclose the effect of a cyber incident on the company's conclusion about the effectiveness of its controls, including that ICFR may be ineffective following or as a result of cyber incident (Item 307 of Reg. S-K)
      ii. Heightened SEC Activity
         1. Initially over 50 SEC comment letters on cybersecurity disclosures
         2. Luis A. Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, *Cyber Risks and the Boardroom*, Conference, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014)[3]
   b. Risk Management Issues
      i. Development and implementation of cybersecurity program
      ii. Response to breach
      iii. Consequences of breach
2. **Internal Controls**
   a. Assist in establishing effective controls (SOX compliance)
   b. Educate board of directors, management and employees
   c. Attorney-client privilege issues

[1] Exhibit A, also available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[2] Exhibit B: Selected Items from Regulation S-K
[3] Exhibit C

i. *Upjohn Co. v. United States*, 449 U.S. 383 (1981)[4]

ii. *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754 (D.C. Circuit 2014)[5]

iii. *In re: Target Corporation Customer Data Security Breach Litigation*, MDL No. 14-2522 (D. Minn. October 23, 2015)[6]

3. Audit Committee

a. Enhanced disclosures for Audit Committees under consideration

i. SEC Concept Release No. 9862, *Possible Revisions to Audit Committee Disclosures* (July 1, 2015)[7]

ii. PCAOB Release No. 2015-004, *Supplemental Request for Comment: Rules to Require Disclosure of Certain Audit Participants on a New PCAOB Form* (June 30, 2015)[8]

iii. PCAOB Release No. 2015-005, *Concept Release on Audit Quality Indicators* (July 1, 2015)[9]

b. Annual evaluation of Audit Committee

c. GC as chief compliance officer

i. Internal management of communications for Audit Committee under ethics policy

ii. Procedures for review and investigation of concerns by and with Audit Committee

This outline was prepared at the request of Jeff Curry, Chief Legal Officer of CBL & Associates Properties, Inc., by Rebecca Taylor of Husch Blackwell LLP, 736 Georgia Avenue, Suite 300, Chattanooga, TN 37402; Phone: 423.755.2662; E-mail: Rebecca.taylor@huschblackwell.com.

[4] Exhibit D
[5] Exhibit E
[6] Exhibit F
[7] Available at http://www.sec.gov/rules/concept/2015/33-9862.pdf
[8] Available at http://pcaobus.org/Rules/Rulemaking/Docket029/Release_2015_004.pdf
[9] Available at http://pcaobus.org/Rules/Rulemaking/Docket%20041/Release_2015_005.pdf

EXHIBIT A

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

Introduction

For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity[1] have also increased, resulting in more frequent and severe cyber incidents. Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. As a result, we determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances.

We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.

In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

The objectives of cyber attacks vary widely and may include theft of financial

assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents

The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.[2] Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.[3] Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

The following sections provide an overview of specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.[4] In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cybersecurity risk disclosure provided must adequately

describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure.[5] Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.

While registrants should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[6] For example, if material intellectual property is stolen in a cyber attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues, an increase in cybersecurity protection costs, including related to litigation, the registrant should discuss these possible outcomes, including the amount and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cybersecurity protection expenditures, the registrant should note those increased expenditures.

Description of Business

If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's "Description of Business."[7] In determining whether to include disclosure, registrants should consider the impact on each of their reportable segments. As an example, if a registrant has a new product in development and learns of a cyber incident that could materially impair its future viability, the registrant should discuss the incident and the potential impact to the extent material.

Legal Proceedings

If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant may need to disclose information regarding this litigation in its "Legal Proceedings" disclosure. For example, if a significant amount of customer information is stolen, resulting in material litigation, the registrant should disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.[8]

Financial Statement Disclosures

Cybersecurity risks and cyber incidents may have a broad impact on a registrant's financial statements, depending on the nature and severity of the potential or actual incident.

Prior to a Cyber Incident

Registrants may incur substantial costs to prevent cyber incidents. Accounting for the capitalization of these costs is addressed by Accounting Standards Codification (ASC) 350-40, *Internal-Use Software*, to the extent that such costs are related to internal use software.

During and After a Cyber Incident

Registrants may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship. Registrants should consider ASC 605-50, *Customer Payments and Incentives*, to ensure appropriate recognition, measurement, and classification of these incentives.

Cyber incidents may result in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts. Registrants should refer to ASC 450-20, *Loss Contingencies*, to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, registrants must provide certain disclosures of losses that are at least reasonably possible.

Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Registrants may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. Registrants should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A registrant must explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be material to the financial statements.[9] Examples of estimates that may be affected by

cyber incidents include estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation, and deferred revenue.

To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, registrants should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary. If the incident constitutes a material nonrecognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.[10]

Disclosure Controls and Procedures

Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.[11] For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.

Endnotes

[1] Cybersecurity is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. Whatis?com available at http://whatis.techtarget.com/definition/cybersecurity.html. See also Merriam-Webster.com available at http://www.merriam-webster.com/dictionary/cybersecurity.

[2] The information in this disclosure guidance is intended to assist registrants in preparing disclosure required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934. In order to maintain the accuracy and completeness of information in effective shelf registration statements, registrants may also need to consider whether it is necessary to file reports on Form 6-K or Form 8-K to disclose the costs and other consequences of material cyber incidents. See Item 5(a) of Form F-3 and Item 11(a) of Form S-3.

[3] Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9. Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available. See Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976). Registrants also should consider the antifraud provisions of the federal securities laws, which apply to statements and omissions both inside and outside of Commission filings. See Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.

[4] See Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

[5] Item 503(c) of Regulation S-K instructs registrants to "not present risks that could apply to any issuer or any offering" and further, to "[e]xplain how the risk affects the issuer or the securities being offered." Item 503(c) of Regulation S-K.

[6] See Item 303 of Regulation S-K; and Form 20-F, Item 5. A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056] Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746]; Management's Discussion and Analysis of Financial Condition and Results of Operations; and Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427].

[7] See Item 101 of Regulation S-K; and Form 20-F, Item 4.B.

[8] See Item 103 of Regulation S-K.

[9] See FASB ASC 275-10, *Risks and Uncertainties.*

[10] See ASC 855-10, *Subsequent Events*.

[11] See Item 307 of Regulation S-K; and Form 20-F, Item 15(a).

http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

EXHIBIT B

§ 229.101 (Item 101) Description of business.

(a) ***General development of business***. Describe the general development of the business of the registrant, its subsidiaries and any predecessor(s) during the past five years, or such shorter period as the registrant may have been engaged in business. Information shall be disclosed for earlier periods if material to an understanding of the general development of the business.

(1) In describing developments, information shall be given as to matters such as the following: the year in which the registrant was organized and its form of organization; the nature and results of any bankruptcy, receivership or similar proceedings with respect to the registrant or any of its significant subsidiaries; the nature and results of any other material reclassification, merger or consolidation of the registrant or any of its significant subsidiaries; the acquisition or disposition of any material amount of assets otherwise than in the ordinary course of business; and any material changes in the mode of conducting the business.

(2) ***Registrants***:

(i) Filing a registration statement on Form S-1 (§ 239.11 of this chapter) under the Securities Act or on Form 10 (§ 249.210 of this chapter) under the Exchange Act;

(ii) Not subject to the reporting requirements of section 13(a) or 15(d) of the Exchange Act immediately before the filing of such registration statement; and

(iii) That (including predecessors) have not received revenue from operations during each of the three fiscal years immediately before the filing of such registration statement, shall provide the following information:

(A) If the registration statement is filed prior to the end of the registrant's second fiscal quarter, a description of the registrant's plan of operation for the remainder of the fiscal year; or

(B) If the registration statement is filed subsequent to the end of the registrant's second fiscal quarter, a descripition of the registrant's plan of operation for the remainder of the fiscal year and for the first six months of the next fiscal year. If such information is not available, the reasons for its not being available shall be stated. Disclosure relating to any plan shall include such matters as:

(*1*) In the case of a registration statement on Form S-1, a statement in narrative form indicating the registrant's opinion as to the period of time that the proceeds from the offering will satisfy cash requirements and whether in the next six months it will be necessary to raise additional funds to meet the expenditures required for operating the business of the registrant; the specific reasons for such opinion shall be set forth and categories of expenditures and sources of cash resources shall be identified; however, amounts of expenditures and cash resources need not be provided; in addition, if the narrative statement is based on a cash budget, such budget shall be furnished to the Commission as supplemental information, but not as part of the registration statement;

(*2*) An explanation of material product research and development to be performed during the period covered in the plan;

(*3*) Any anticipated material acquisition of plant and equipment and the capacity thereof;

(*4*) Any anticipated material changes in number of employees in the various departments such as research and development, production, sales or administration; and

(*5*) Other material areas which may be peculiar to the registrant's business.

(b) ***Financial information about segments***. Report for each segment, as defined by generally accepted accounting principles, revenues from external customers, a measure of profit or loss and total assets. A registrant must report this information for each of the last three fiscal years or for as long as it has been in business, whichever period is shorter. If the information provided in response to this paragraph (b) conforms with generally accepted accounting principles, a registrant may include in its financial statements a cross reference to this data in lieu of presenting duplicative information in the financial statements; conversely, a registrant may cross reference to the financial statements.

(1) If a registrant changes the structure of its internal organization in a manner that causes the composition of its reportable segments to change, the registrant must restate the corresponding information for earlier periods, including interim periods, unless it is impracticable to do so. Following a change in the composition of its reportable segments, a registrant shall disclose whether it has restated the corresponding items of segment information for earlier periods. If it has not restated the items from earlier periods, the registrant shall disclose in the year in which the change occurs segment information for the current period under both the old basis and the new basis of segmentation, unless it is impracticable to do so.

(2) If the registrant includes, or is required by Article 3 of Regulation S-X (17 CFR 210) to include, interim financial statements, discuss any facts relating to the performance of any of the segments during the period which, in the opinion of management, indicate that the three year segment financial data may not be indicative of current or future operations

of the segment. Comparative financial information shall be included to the extent necessary to the discussion.

(c) ***Narrative description of business***.

(1) Describe the business done and intended to be done by the registrant and its subsidiaries, focusing upon the registrant's dominant segment or each reportable segment about which financial information is presented in the financial statements. To the extent material to an understanding of the registrant's business taken as a whole, the description of each such segment shall include the information specified in paragraphs (c)(1) (i) through (x) of this section. The matters specified in paragraphs (c)(1) (xi) through (xiii) of this section shall be discussed with respect to the registrant's business in general; where material, the segments to which these matters are significant shall be identified.

(i) The principal products produced and services rendered by the registrant in the segment and the principal markets for, and methods of distribution of, the segment's principal products and services. In addition, state for each of the last three fiscal years the amount or percentage of total revenue contributed by any class of similar products or services which accounted for 10 percent or more of consolidated revenue in any of the last three fiscal years or 15 percent or more of consolidated revenue, if total revenue did not exceed $50,000,000 during any of such fiscal years.

(ii) A description of the status of a product or segment (e.g. whether in the planning stage, whether prototypes exist, the degree to which product design has progressed or whether further engineering is necessary), if there has been a public announcement of, or if the registrant otherwise has made public information about, a new product or segment that would require the investment of a material amount of the assets of the registrant or that otherwise is material. This paragraph is not intended to require disclosure of otherwise nonpublic corporate information the disclosure of which would affect adversely the registrant's competitive position.

(iii) ***The sources and availability of raw materials***.

(iv) The importance to the segment and the duration and effect of all patents, trademarks, licenses, franchises and concessions held.

(v) The extent to which the business of the segment is or may be seasonal.

(vi) The practices of the registrant and the industry (respective industries) relating to working capital items (e.g., where the registrant is required to carry significant amounts of inventory to meet rapid delivery requirements of customers or to assure itself of a continuous allotment of goods from suppliers; where the registrant provides rights to return merchandise; or where the registrant has provided extended payment terms to customers).

(vii) The dependence of the segment upon a single customer, or a few customers, the loss of any one or more of which would have a material adverse effect on the segment. The name of any customer and its relationship, if any, with the registrant or its subsidiaries shall be disclosed if sales to the customer by one or more segments are made in an aggregate amount equal to 10 percent or more of the registrant's consolidated revenues and the loss of such customer would have a material adverse effect on the registrant and its subsidiaries taken as a whole. The names of other customers may be included, unless in the particular case the effect of including the names would be misleading. For purposes of this paragraph, a group of customers under common control or customers that are affiliates of each other shall be regarded as a single customer.

(viii) The dollar amount of backlog orders believed to be firm, as of a recent date and as of a comparable date in the preceding fiscal year, together with an indication of the portion thereof not reasonably expected to be filled within the current fiscal year, and seasonal or other material aspects of the backlog. (There may be included as firm orders government orders that are firm but not yet funded and contracts awarded but not yet signed, provided an appropriate statement is added to explain the nature of such orders and the amount thereof. The portion of orders already included in sales or operating revenues on the basis of percentage of completion or program accounting shall be excluded.)

(ix) A description of any material portion of the business that may be subject to renegotiation of profits or termination of contracts or subcontracts at the election of the Government.

(x) Competitive conditions in the business involved including, where material, the identity of the particular markets in which the registrant competes, an estimate of the number of competitors and the registrant's competitive position, if known or reasonably available to the registrant. Separate consideration shall be given to the principal products or services or classes of products or services of the segment, if any. Generally, the names of competitors need not be disclosed. The registrant may include such names, unless in the particular case the effect of including the names would be misleading. Where, however, the registrant knows or has reason to know that one or a small number of competitors is dominant in the industry it shall be identified. The principal methods of competition (e.g., price, service, warranty or product performance) shall be identified, and positive and negative factors pertaining to the competitive position of the registrant, to the extent that they exist, shall be explained if known or reasonably available to the registrant.

(xi) If material, the estimated amount spent during each of the last three fiscal years on company-sponsored research and development activities determined in accordance with generally accepted accounting principles. In addition, state, if material, the estimated dollar amount spent during each of such years on customer-sponsored

research activities relating to the development of new products, services or techniques or the improvement of existing products, services or techniques.

(xii) Appropriate disclosure also shall be made as to the material effects that compliance with Federal, State and local provisions which have been enacted or adopted regulating the discharge of materials into the environment, or otherwise relating to the protection of the environment, may have upon the capital expenditures, earnings and competitive position of the registrant and its subsidiaries. The registrant shall disclose any material estimated capital expenditures for environmental control facilities for the remainder of its current fiscal year and its succeeding fiscal year and for such further periods as the registrant may deem materials.

(xiii) ***The number of persons employed by the registrant***.

(d) ***Financial information about geographic areas***.

(1) State for each of the registrant's last three fiscal years, or for each fiscal year the registrant has been engaged in business, whichever period is shorter:

(i) ***Revenues from external customers attributed to***:

(A) ***The registrant's country of domicile***;

(B) All foreign countries, in total, from which the registrant derives revenues; and

(C) ***Any individual foreign country, if material***. Disclose the basis for attributing revenues from external customers to individual countries.

(ii) Long-lived assets, other than financial instruments, long-term customer relationships of a financial institution, mortgage and other servicing rights, deferred policy acquisition costs, and deferred tax assets, located in:

(A) ***The registrant's country of domicile***;

(B) All foreign countries, in total, in which the registrant holds assets; and

(C) ***Any individual foreign country, if material***.

(2) A registrant shall report the amounts based on the financial information that it uses to produce the general-purpose financial statements. If providing the geographic information is impracticable, the registrant shall disclose that fact. A registrant may wish to provide, in addition to the information required by paragraph (d)(1) of this section, subtotals of geographic information about groups of countries. To the extent that the disclosed information conforms with generally accepted accounting principles, the registrant may include in its financial statements a cross reference to this data in lieu of presenting duplicative data in its financial statements; conversely, a registrant may cross-reference to the financial statements.

(3) A registrant shall describe any risks attendant to the foreign operations and any dependence on one or more of the registrant's segments upon such foreign operations, unless it would be more appropriate to discuss this information in connection with the description of one or more of the registrant's segments under paragraph (c) of this item.

(4) If the registrant includes, or is required by Article 3 of Regulation S-X (17 CFR 210), to include, interim financial statements, discuss any facts relating to the information furnished under this paragraph (d) that, in the opinion of management, indicate that the three year financial data for geographic areas may not be indicative of current or future operations. To the extent necessary to the discussion, include comparative information.

(e) ***Available information***. Disclose the information in paragraphs (e)(1), (e)(2) and (e)(3) of this section in any registration statement you file under the Securities Act (15 U.S.C. 77a *et seq.*), and disclose the information in paragraphs (e)(3) and (e)(4) of this section if you are an accelerated filer or a large accelerated filer (as defined in § 240.12b-2 of this chapter) filing an annual report on Form 10-K (§ 249.310 of this chapter):

(1) Whether you file reports with the Securities and Exchange Commission. If you are a reporting company, identify the reports and other information you file with the SEC.

(2) That the public may read and copy any materials you file with the SEC at the SEC's Public Reference Room at 100 F Street, NE., Washington, DC 20549. State that the public may obtain information on the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. If you are an electronic filer, state that the SEC maintains an Internet site that contains reports, proxy and information statements, and other information regarding issuers that file electronically with the SEC and state the address of that site (*http://www.sec.gov*).

(3) You are encouraged to give your Internet address, if available, except that if you are an accelerated filer or a large accelerated filer filing your annual report on Form 10-K, you must disclose your Internet address, if you have one.

(4)

(i) Whether you make available free of charge on or through your Internet website, if you have one, your annual report on Form 10-K, quarterly reports on Form 10-Q (§ 249.308a of this chapter), current reports on Form 8-K

(§ 249.308 of this chapter), and amendments to those reports filed or furnished pursuant to Section 13(a) or 15(d) of the Exchange Act (15 U.S.C. 78m(a) or 78o(d)) as soon as reasonably practicable after you electronically file such material with, or furnish it to, the SEC;

(ii) If you do not make your filings available in this manner, the reasons you do not do so (including, where applicable, that you do not have an Internet website); and

(iii) If you do not make your filings available in this manner, whether you voluntarily will provide electronic or paper copies of your filings free of charge upon request.

(f) ***Reports to security holders***. Disclose the following information in any registration statement you file under the Securities Act:

(1) If the SEC's proxy rules or regulations, or stock exchange requirements, do not require you to send an annual report to security holders or to holders of American depository receipts, describe briefly the nature and frequency of reports that you will give to security holders. Specify whether the reports that you give will contain financial information that has been examined and reported on, with an opinion expressed "by" an independent public or certified public accountant.

(2) For a foreign private issuer, if the report will not contain financial information prepared in accordance with U.S. generally accepted accounting principles, you must state whether the report will include a reconciliation of this information with U.S. generally accepted accounting principles.

(g) ***Enforceability of civil liabilities against foreign persons***. Disclose the following if you are a foreign private issuer filing a registration statement under the Securities Act:

(1) Whether or not investors may bring actions under the civil liability provisions of the U.S. Federal securities laws against the foreign private issuer, any of its officers and directors who are residents of a foreign country, any underwriters or experts named in the registration statement that are residents of a foreign country, and whether investors may enforce these civil liability provisions when the assets of the issuer or these other persons are located outside of the United States. The disclosure must address the following matters:

(i) The investor's ability to effect service of process within the United States on the foreign private issuer or any person;

(ii) The investor's ability to enforce judgments obtained in U.S. courts against foreign persons based upon the civil liability provisions of the U.S. Federal securities laws;

(iii) The investor's ability to enforce, in an appropriate foreign court, judgments of U.S. courts based upon the civil liability provisions of the U.S. Federal securities laws; and

(iv) The investor's ability to bring an original action in an appropriate foreign court to enforce liabilities against the foreign private issuer or any person based upon the U.S. Federal securities laws.

(2) If you provide this disclosure based on an opinion of counsel, name counsel in the prospectus and file as an exhibit to the registration statement a signed consent of counsel to the use of its name and opinion.

(h) ***Smaller reporting companies*** . A smaller reporting company, as defined by § 229.10(f)(1), may satisfy its obligations under this Item by describing the development of its business during the last three years. If the smaller reporting company has not been in business for three years, give the same information for predecessor(s) of the smaller reporting company if there are any. This business development description should include:

(1) ***Form and year of organization***;

(2) Any bankruptcy, receivership or similar proceeding; and

(3) Any material reclassification, merger, consolidation, or purchase or sale of a significant amount of assets not in the ordinary course of business.

(4) ***Business of the smaller reporting company*** . Briefly describe the business and include, to the extent material to an understanding of the smaller reporting company:

(i) Principal products or services and their markets;

(ii) Distribution methods of the products or services;

(iii) Status of any publicly announced new product or service;

(iv) Competitive business conditions and the smaller reporting company's competitive position in the industry and methods of competition;

(v) Sources and availability of raw materials and the names of principal suppliers;

(vi) Dependence on one or a few major customers;

(vii) Patents, trademarks, licenses, franchises, concessions, royalty agreements or labor contracts, including duration;

(viii) Need for any government approval of principal products or services. If government approval is necessary and the smaller reporting company has not yet received that approval, discuss the status of the approval within the government approval process;

(ix) Effect of existing or probable governmental regulations on the business;

(x) Estimate of the amount spent during each of the last two fiscal years on research and development activities, and if applicable, the extent to which the cost of such activities is borne directly by customers;

(xi) Costs and effects of compliance with environmental laws (federal, state and local); and

(xii) Number of total employees and number of full-time employees.

(5) ***Reports to security holders*** . Disclose the following in any registration statement you file under the Securities Act of 1933:

(i) If you are not required to deliver an annual report to security holders, whether you will voluntarily send an annual report and whether the report will include audited financial statements;

(ii) Whether you file reports with the Securities and Exchange Commission. If you are a reporting company, identify the reports and other information you file with the Commission; and

(iii) That the public may read and copy any materials you file with the Commission at the SEC's Public Reference Room at 100 F Street, NE., Washington, DC 20549, on official business days during the hours of 10 a.m. to 3 p.m. State that the public may obtain information on the operation of the Public Reference Room by calling the Commission at 1-800-SEC-0330. State that the Commission maintains an Internet site that contains reports, proxy and information statements, and other information regarding issuers that file electronically with the Commission and state the address of that site (*http://www.sec.gov*). You are encouraged to give your Internet address, if available.

(6) ***Foreign issuers*** . Provide the information required by Item 101(g) of Regulation S-K (§ 229.101(g)).

Instructions to Item 101*:*

1. In determining what information about the segments is material to an understanding of the registrant's business taken as a whole and therefore required to be disclosed, pursuant to paragraph (c) of this Item, the registrant should take into account both quantitative and qualitative factors such as the significance of the matter to the registrant (e.g., whether a matter with a relatively minor impact on the registrant's business is represented by management to be important to its future profitability), the pervasiveness of the matter (e.g., whether it affects or may affect numerous items in the segment information), and the impact of the matter (e.g., whether it distorts the trends reflected in the segment information). Situations may arise when information should be disclosed about a segment, although the information in quantitative terms may not appear significant to the registrant's business taken as a whole.

2. Base the determination of whether information about segments is required for a particular year upon an evaluation of interperiod comparability. For instance, interperiod comparability would require a registrant to report segment information in the current period even if not material under the criteria for reportability of FASB ASC Topic 280, *Segment Reporting,* if a segment has been significant in the immediately preceding period and the registrant expects it to be significant in the future.

3. The Commission, upon written request of the registrant and where consistent with the protection of investors, may permit the omission of any of the information required by this Item or the furnishing in substitution thereof of appropriate information of comparable character.

[47 FR 11401, Mar. 16, 1982, as amended at 63 FR 6381, Feb. 6, 1998; 64 FR 1734, Jan. 12, 1999; 67 FR 58504, Sept. 16, 2002; 70 FR 76641, Dec. 27, 2005; 73 FR 957, Jan. 4, 2008; 76 FR 50120, Aug. 12, 2011]

§ 229.103 (Item 103) Legal proceedings.

Describe briefly any material pending legal proceedings, other than ordinary routine litigation incidental to the business, to which the registrant or any of its subsidiaries is a party or of which any of their property is the subject. Include the name of the court or agency in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the proceeding and the relief sought. Include similar information as to any such proceedings known to be contemplated by governmental authorities.

***Instructions to Item 103**:*

1. If the business ordinarily results in actions for negligence or other claims, no such action or claim need be described unless it departs from the normal kind of such actions.

2. No information need be given with respect to any proceeding that involves primarily a claim for damages if the amount involved, exclusive of interest and costs, does not exceed 10 percent of the current assets of the registrant and its subsidiaries on a consolidated basis. However, if any proceeding presents in large degree the same legal and factual issues as other proceedings pending or known to be contemplated, the amount involved in such other proceedings shall be included in computing such percentage.

3. Notwithstanding Instructions 1 and 2, any material bankruptcy, receivership, or similar proceeding with respect to the registrant or any of its significant subsidiaries shall be described.

4. Any material proceedings to which any director, officer or affiliate of the registrant, any owner of record or beneficially of more than five percent of any class of voting securities of the registrant, or any associate of any such director, officer, affiliate of the registrant, or security holder is a party adverse to the registrant or any of its subsidiaries or has a material interest adverse to the registrant or any of its subsidiaries also shall be described.

5. Notwithstanding the foregoing, an administrative or judicial proceeding (including, for purposes of A and B of this Instruction, proceedings which present in large degree the same issues) arising under any Federal, State or local provisions that have been enacted or adopted regulating the discharge of materials into the environment or primary for the purpose of protecting the environment shall not be deemed "ordinary routine litigation incidental to the business" and shall be described if:

A. Such proceeding is material to the business or financial condition of the registrant;

B. Such proceeding involves primarily a claim for damages, or involves potential monetary sanctions, capital expenditures, deferred charges or charges to income and the amount involved, exclusive of interest and costs, exceeds 10 percent of the current assets of the registrant and its subsidiaries on a consolidated basis; or

C. A governmental authority is a party to such proceeding and such proceeding involves potential monetary sanctions, unless the registrant reasonably believes that such proceeding will result in no monetary sanctions, or in monetary sanctions, exclusive of interest and costs, of less than $100,000; provided, however, that such proceedings which are similar in nature may be grouped and described generically.

§ 229.303 (Item 303) Management's discussion and analysis of financial condition and results of operations.

(a) ***Full fiscal years.*** Discuss registrant's financial condition, changes in financial condition and results of operations. The discussion shall provide information as specified in paragraphs (a)(1) through (5) of this Item and also shall provide such other information that the registrant believes to be necessary to an understanding of its financial condition, changes in financial condition and results of operations. Discussions of liquidity and capital resources may be combined whenever the two topics are interrelated. Where in the registrant's judgment a discussion of segment information or of other subdivisions of the registrant's business would be appropriate to an understanding of such business, the discussion shall focus on each relevant, reportable segment or other subdivision of the business and on the registrant as a whole.

(1) ***Liquidity.*** Identify any known trends or any known demands, commitments, events or uncertainties that will result in or that are reasonably likely to result in the registrant's liquidity increasing or decreasing in any material way. If a material deficiency is identified, indicate the course of action that the registrant has taken or proposes to take to remedy the deficiency. Also identify and separately describe internal and external sources of liquidity, and briefly discuss any material unused sources of liquid assets.

(2) ***Capital resources.***

(i) Describe the registrant's material commitments for capital expenditures as of the end of the latest fiscal period, and indicate the general purpose of such commitments and the anticipated source of funds needed to fulfill such commitments.

(ii) Describe any known material trends, favorable or unfavorable, in the registrant's capital resources. Indicate any expected material changes in the mix and relative cost of such resources. The discussion shall consider changes between equity, debt and any off-balance sheet financing arrangements.

(3) ***Results of operations.***

(i) Describe any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations and, in each case, indicate the extent to which income was so affected. In addition, describe any other significant components of revenues or expenses that, in the registrant's judgment, should be described in order to understand the registrant's results of operations.

(ii) Describe any known trends or uncertainties that have had or that the registrant reasonably expects will have a material favorable or unfavorable impact on net sales or revenues or income from continuing operations. If the registrant knows of events that will cause a material change in the relationship between costs and revenues (such as known future increases in costs of labor or materials or price increases or inventory adjustments), the change in the relationship shall be disclosed.

(iii) To the extent that the financial statements disclose material increases in net sales or revenues, provide a narrative discussion of the extent to which such increases are attributable to increases in prices or to increases in the volume or amount of goods or services being sold or to the introduction of new products or services.

(iv) For the three most recent fiscal years of the registrant or for those fiscal years in which the registrant has been engaged in business, whichever period is shortest, discuss the impact of inflation and changing prices on the registrant's net sales and revenues and on income from continuing operations.

(4) ***Off-balance sheet arrangements.***

(i) In a separately-captioned section, discuss the registrant's off-balance sheet arrangements that have or are reasonably likely to have a current or future effect on the registrant's financial condition, changes in financial condition, revenues or expenses, results of operations, liquidity, capital expenditures or capital resources that is material to investors. The disclosure shall include the items specified in paragraphs (a)(4)(i)(A), (B), (C) and (D) of this Item to the extent necessary to an understanding of such arrangements and effect and shall also include such other information that the registrant believes is necessary for such an understanding.

(A) The nature and business purpose to the registrant of such off-balance sheet arrangements;

(B) The importance to the registrant of such off-balance sheet arrangements in respect of its liquidity, capital resources, market risk support, credit risk support or other benefits;

(C) The amounts of revenues, expenses and cash flows of the registrant arising from such arrangements; the nature and amounts of any interests retained, securities issued and other indebtedness incurred by the registrant in connection with such arrangements; and the nature and amounts of any other obligations or liabilities (including contingent obligations or liabilities) of the registrant arising from such arrangements that are or are reasonably likely to become material and the triggering events or circumstances that could cause them to arise; and

(D) Any known event, demand, commitment, trend or uncertainty that will result in or is reasonably likely to result in the termination, or material reduction in availability to the registrant, of its off-balance sheet arrangements that

provide material benefits to it, and the course of action that the registrant has taken or proposes to take in response to any such circumstances.

(ii) ***As used in this paragraph (a)(4), the term*** *off-balance sheet arrangement* means any transaction, agreement or other contractual arrangement to which an entity unconsolidated with the registrant is a party, under which the registrant has:

(A) Any obligation under a guarantee contract that has any of the characteristics identified in FASB ASC paragraph 460-10-15-4 (Guarantees Topic), as may be modified or supplemented, and that is not excluded from the initial recognition and measurement provisions of FASB ASC paragraphs 460-10-15-7, 460-10-25-1, and 460-10-30-1.

(B) A retained or contingent interest in assets transferred to an unconsolidated entity or similar arrangement that serves as credit, liquidity or market risk support to such entity for such assets;

(C) Any obligation, including a contingent obligation, under a contract that would be accounted for as a derivative instrument, except that it is both indexed to the registrant's own stock and classified in stockholders' equity in the registrant's statement of financial position, and therefore excluded from the scope of FASB ASC Topic 815, *Derivatives and Hedging,* pursuant to FASB ASC subparagraph 815-10-15-74(a), as may be modified or supplemented; or

(D) Any obligation, including a contingent obligation, arising out of a variable interest (as defined in the FASB ASC Master Glossary), as may be modified or supplemented) in an unconsolidated entity that is held by, and material to, the registrant, where such entity provides financing, liquidity, market risk or credit risk support to, or engages in leasing, hedging or research and development services with, the registrant.

(5) ***Tabular disclosure of contractual obligations****.*

(i) In a tabular format, provide the information specified in this paragraph (a)(5) as of the latest fiscal year end balance sheet date with respect to the registrant's known contractual obligations specified in the table that follows this paragraph (a)(5)(i). The registrant shall provide amounts, aggregated by type of contractual obligation. The registrant may disaggregate the specified categories of contractual obligations using other categories suitable to its business, but the presentation must include all of the obligations of the registrant that fall within the specified categories. A presentation covering at least the periods specified shall be included. The tabular presentation may be accompanied by footnotes to describe provisions that create, increase or accelerate obligations, or other pertinent data to the extent necessary for an understanding of the timing and amount of the registrant's specified contractual obligations.

Contractual obligations	Payments due by period			3-5 years	More than 5 years
	Total	Less than 1 year	1-3 years		
[Long-Term Debt Obligations]					
[Capital Lease Obligations]					
[Operating Lease Obligations]					
[Purchase Obligations]					
[Other Long-Term Liabilities Reflected on the Registrant's Balance Sheet under GAAP]					
Total					

(ii) ***Definitions****:* The following definitions apply to this paragraph (a)(5):

(A) ***Long-term debt obligation*** means a payment obligation under long-term borrowings referenced in FASB ASC paragraph 470-10-50-1 (Debt Topic), as may be modified or supplemented.

(B) ***Capital lease obligation*** means a payment obligation under a lease classified as a capital lease pursuant to FASB ASC Topic 840, *Leases".* , as may be modified or supplemented.

(C) ***Operating lease obligation*** means a payment obligation under a lease classified as an operating lease and disclosed pursuant to FASB ASC Topic 840, as may be modified or supplemented.

(D) ***Purchase obligation*** means an agreement to purchase goods or services that is enforceable and legally binding on the registrant that specifies all significant terms, including: fixed or minimum quantities to be purchased; fixed, minimum or variable price provisions; and the approximate timing of the transaction.

Instructions to paragraph 303(a): 1. The registrant's discussion and analysis shall be of the financial statements and other statistical data that the registrant believes will enhance a reader's understanding of its financial condition, changes in financial condition and results of operations. Generally, the discussion shall cover the three-year period covered by the

financial statements and shall use year-to-year comparisons or any other formats that in the registrant's judgment enhance a reader's understanding. However, where trend information is relevant, reference to the five-year selected financial data appearing pursuant to Item 301 of Regulation S-K (§ 229.301) may be necessary. A smaller reporting company's discussion shall cover the two-year period required in Article 8 of Regulation S-X and shall use year-to-year comparisons or any other formats that in the registrant's judgment enhance a reader's understanding.

2. The purpose of the discussion and analysis shall be to provide to investors and other users information relevant to an assessment of the financial condition and results of operations of the registrant as determined by evaluating the amounts and certainty of cash flows from operations and from outside sources.

3. The discussion and analysis shall focus specifically on material events and uncertainties known to management that would cause reported financial information not to be necessarily indicative of future operating results or of future financial condition. This would include descriptions and amounts of (A) matters that would have an impact on future operations and have not had an impact in the past, and (B) matters that have had an impact on reported operations and are not expected to have an impact upon future operations.

4. Where the consolidated financial statements reveal material changes from year to year in one or more line items, the causes for the changes shall be described to the extent necesary to an understanding of the registrant's businesses as a whole; *Provided, however,* That if the causes for a change in one line item also relate to other line items, no repetition is required and a line-by-line analysis of the financial statements as a whole is not required or generally appropriate. Registrants need not recite the amounts of changes from year to year which are readily computable from the financial statements. The discussion shall not merely repeat numerical data contained in the consolidated financial statements.

5. The term "liquidity" as used in this Item refers to the ability of an enterprise to generate adequate amounts of cash to meet the enterprise's needs for cash. Except where it is otherwise clear from the discussion, the registrant shall indicate those balance sheet conditions or income or cash flow items which the registrant believes may be indicators of its liquidity condition. Liquidity generally shall be discussed on both a long-term and short-term basis. The issue of liquidity shall be discussed in the context of the registrant's own business or businesses. For example a discussion of working capital may be appropriate for certain manufacturing, industrial or related operations but might be inappropriate for a bank or public utility.

6. Where financial statements presented or incorporated by reference in the registration statement are required by § 210.4-08(e)(3) of Regulation S-X [17 CFR part 210] to include disclosure of restrictions on the ability of both consolidated and unconsolidated subsidiaries to transfer funds to the registrant in the form of cash dividends, loans or advances, the discussion of liquidity shall include a discussion of the nature and extent of such restrictions and the impact such restrictions have had and are expected to have on the ability of the parent company to meet its cash obligations.

7. Any forward-looking information supplied is expressly covered by the safe harbor rule for projections. See Rule 175 under the Securities Act [17 CFR 230.175], Rule 3b-6 under the Exchange Act [17 CFR 240.3b-6] and Securities Act Release No. 6084 (June 25, 1979) (44 FR 38810).

8. Registrants are only required to discuss the effects of inflation and other changes in prices when considered material. This discussion may be made in whatever manner appears appropriate under the circumstances. All that is required is a brief textual presentation of management's views. No specific numerical financial data need be presented except as Rule 3-20(c) of Regulation S-X (§ 210.3-20(c) of this chapter) otherwise requires. However, registrants may elect to voluntarily disclose supplemental information on the effects of changing prices as provided for in FASB ASC Topic 255, *Changing Prices,* or through other supplemental disclosures. The Commission encourages experimentation with these disclosures in order to provide the most meaningful presentation of the impact of price changes on the registrant's financial statements.

9. Registrants that elect to disclose supplementary information on the effects of changing prices as specified by FASB ASC Topic 255 may combine such explanations with the discussion and analysis required pursuant to this Item or may supply such information separately with appropriate cross reference.

10. All references to the registrant in the discussion and in this Item shall mean the registrant and its subsidiaries consolidated.

11. Foreign private registrants also shall discuss briefly any pertinent governmental economic, fiscal, monetary, or political policies or factors that have materially affected or could materially affect, directly or indirectly, their operations or investments by United States nationals.

12. If the registrant is a foreign private issuer, the discussion shall focus on the primary financial statements presented in the registration statement or report. There shall be a reference to the reconciliation to United States generally accepted accounting principles, and a discussion of any aspects of the difference between foreign and United States generally accepted accounting principles, not discussed in the reconciliation, that the registrant believes is necessary for an understanding of the financial statements as a whole.

13. The attention of bank holding companies is directed to the information called for in Guide 3 (§ 229.801(c) and § 229.802(c)).

14. The attention of property-casualty insurance companies is directed to the information called for in Guide 6 (§ 229.801(f)).

Instructions to paragraph 303(a)(4): 1. No obligation to make disclosure under paragraph (a)(4) of this Item shall arise in respect of an off-balance sheet arrangement until a definitive agreement that is unconditionally binding or subject only to customary closing conditions exists or, if there is no such agreement, when settlement of the transaction occurs.

2. Registrants should aggregate off-balance sheet arrangements in groups or categories that provide material information in an efficient and understandable manner and should avoid repetition and disclosure of immaterial information. Effects that are common or similar with respect to a number of off-balance sheet arrangements must be analyzed in the aggregate to the extent the aggregation increases understanding. Distinctions in arrangements and their effects must be discussed to the extent the information is material, but the discussion should avoid repetition and disclosure of immaterial information.

3. For purposes of paragraph (a)(4) of this Item only, contingent liabilities arising out of litigation, arbitration or regulatory actions are not considered to be off-balance sheet arrangements.

4. Generally, the disclosure required by paragraph (a)(4) shall cover the most recent fiscal year. However, the discussion should address changes from the previous year where such discussion is necessary to an understanding of the disclosure.

5. In satisfying the requirements of paragraph (a)(4) of this Item, the discussion of off-balance sheet arrangements need not repeat information provided in the footnotes to the financial statements, provided that such discussion clearly cross-references to specific information in the relevant footnotes and integrates the substance of the footnotes into such discussion in a manner designed to inform readers of the significance of the information that is not included within the body of such discussion.

(b) ***Interim periods***. If interim period financial statements are included or are required to be included by Article 3 of Regulation S-X (17 CFR 210), a management's discussion and analysis of the financial condition and results of operations shall be provided so as to enable the reader to assess material changes in financial condition and results of operations between the periods specified in paragraphs (b) (1) and (2) of this Item. The discussion and analysis shall include a discussion of material changes in those items specifically listed in paragraph (a) of this Item, except that the impact of inflation and changing prices on operations for interim periods need not be addressed.

(1) ***Material changes in financial condition***. Discuss any material changes in financial condition from the end of the preceding fiscal year to the date of the most recent interim balance sheet provided. If the interim financial statements include an interim balance sheet as of the corresponding interim date of the preceding fiscal year, any material changes in financial condition from that date to the date of the most recent interim balance sheet provided also shall be discussed. If discussions of changes from both the end and the corresponding interim date of the preceding fiscal year are required, the discussions may be combined at the discretion of the registrant.

(2) ***Material changes in results of operations***. Discuss any material changes in the registrant's results of operations with respect to the most recent fiscal year-to-date period for which an income statement is provided and the corresponding year-to-date period of the preceding fiscal year. If the registrant is required to or has elected to provide an income statement for the most recent fiscal quarter, such discussion also shall cover material changes with respect to that fiscal quarter and the corresponding fiscal quarter in the preceding fiscal year. In addition, if the registrant has elected to provide an income statement for the twelve-month period ended as of the date of the most recent interim balance sheet provided, the discussion also shall cover material changes with respect to that twelve-month period and the twelve-month period ended as of the corresponding interim balance sheet date of the preceding fiscal year. Notwithstanding the above, if for purposes of a registration statement a registrant subject to paragraph (b) of § 210.3-03 of Regulation S-X provides a statement of income for the twelve-month period ended as of the date of the most recent interim balance sheet provided in lieu of the interim income statements otherwise required, the discussion of material changes in that twelve-month period will be in respect to the preceding fiscal year rather than the corresponding preceding period.

Instructions to paragraph (b) of Item 303*:*

1. If interim financial statements are presented together with financial statements for full fiscal years, the discussion of the interim financial information shall be prepared pursuant to this paragraph (b) and the discussion of the full fiscal year's information shall be prepared pursuant to paragraph (a) of this Item. Such discussions may be combined.

2. In preparing the discussion and analysis required by this paragraph (b), the registrant may presume that users of the interim financial information have read or have access to the discussion and analysis required by paragraph (a) for the preceding fiscal year.

3. The discussion and analysis required by this paragraph (b) is required to focus only on material changes. Where the interim financial statements reveal material changes from period to period in one or more significant line items, the causes for the changes shall be described if they have not already been disclosed: *Provided, however,* That if the causes for a change in one line item also relate to other line items, no repetition is required. Registrants need not recite the amounts of changes from period to period which are readily computable from the financial statements. The discussion shall not merely repeat numerical data contained in the financial statements. The information provided shall include that which is available to the registrant without undue effort or expense and which does not clearly appear in the registrant's condensed interim financial statements.

4. The registrant's discussion of material changes in results of operations shall identify any significant elements of the registrant's income or loss from continuing operations which do not arise from or are not necessarily representative of the registrant's ongoing business.

5. The registrant shall discuss any seasonal aspects of its business which have had a material effect upon its financial condition or results of operation.

6. Any forward-looking information supplied is expressly covered by the safe harbor rule for projections. See Rule 175 under the Securities Act [17 CFR 230. 175], Rule 3b-6 under the Exchange Act [17 CFR 249.3b-6] and Securities Act Release No. 6084 (June 25, 1979) (44 FR 38810).

7. The registrant is not required to include the table required by paragraph (a)(5) of this Item for interim periods. Instead, the registrant should disclose material changes outside the ordinary course of the registrant's business in the specified contractual obligations during the interim period.

(c) ***Safe harbor***.

(1) The safe harbor provided in section 27A of the Securities Act of 1933 (15 U.S.C. 77z-2) and section 21E of the Securities Exchange Act of 1934 (15 U.S.C. 78u-5) ("statutory safe harbors") shall apply to forward-looking information provided pursuant to paragraphs (a)(4) and (5) of this Item, provided that the disclosure is made by: an issuer; a person acting on behalf of the issuer; an outside reviewer retained by the issuer making a statement on behalf of the issuer; or an underwriter, with respect to information provided by the issuer or information derived from information provided by the issuer.

(2) ***For purposes of paragraph (c) of this Item only***:

(i) All information required by paragraphs (a)(4) and (5) of this Item is deemed to be a *forward looking statement* as that term is defined in the statutory safe harbors, except for historical facts.

(ii) With respect to paragraph (a)(4) of this Item, the meaningful cautionary statements element of the statutory safe harbors will be satisfied if a registrant satisfies all requirements of that same paragraph (a)(4) of this Item.

(d) ***Smaller reporting companies*** . A smaller reporting company, as defined by § 229.10(f)(1), may provide the information required in paragraph (a)(3)(iv) of this Item for the last two most recent fiscal years of the registrant if it provides financial information on net sales and revenues and on income from continuing operations for only two years. A smaller reporting company is not required to provide the information required by paragraph (a)(5) of this Item.

[47 FR 11401, Mar. 16, 1982, as amended at 47 FR 29839, July 9, 1982; 47 FR 54768, Dec. 6, 1982; 52 FR 30919, Aug. 18, 1987; 68 FR 5999, Feb. 5, 2003; 73 FR 958, Jan. 4, 2008; 76 FR 50120, Aug. 12, 2011]

§ 229.307 (Item 307) Disclosure controls and procedures.

Disclose the conclusions of the registrant's principal executive and principal financial officers, or persons performing similar functions, regarding the effectiveness of the registrant's disclosure controls and procedures (as defined in § 240.13a-15(e) or § 240.15d-15(e) of this chapter) as of the end of the period covered by the report, based on the evaluation of these controls and procedures required by paragraph (b) of § 240.13a-15 or § 240.15d-15 of this chapter.

[68 FR 36663, June 18, 2003]

§ 229.503 (Item 503) Prospectus summary, risk factors, and ratio of earnings to fixed charges.

The registrant must furnish this information in plain English. See § 230.421(d) of Regulation C of this chapter.

(a) ***Prospectus summary***. Provide a summary of the information in the prospectus where the length or complexity of the prospectus makes a summary useful. The summary should be brief. The summary should not contain, and is not required to contain, all of the detailed information in the prospectus. If you provide summary business or financial information, even if you do not caption it as a summary, you still must provide that information in plain English.

Instruction to paragraph 503(a): The summary should not merely repeat the text of the prospectus but should provide a brief overview of the key aspects of the offering. Carefully consider and identify those aspects of the offering that are the most significant and determine how best to highlight those points in clear, plain language.

(b) ***Address and telephone number***. Include, either on the cover page or in the summary section of the prospectus, the complete mailing address and telephone number of your principal executive offices.

(c) ***Risk factors***. Where appropriate, provide under the caption "Risk Factors" a discussion of the most significant factors that make the offering speculative or risky. This discussion must be concise and organized logically. Do not present risks that could apply to any issuer or any offering. Explain how the risk affects the issuer or the securities being offered. Set forth each risk factor under a subcaption that adequately describes the risk. The risk factor discussion must immediately follow the summary section. If you do not include a summary section, the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page. Pricing information means price and price-related information that you may omit from the prospectus in an effective registration statement based on § 230.430A(a) of this chapter. The risk factors may include, among other things, the following:

(1) ***Your lack of an operating history***;

(2) Your lack of profitable operations in recent periods;

(3) ***Your financial position***;

(4) ***Your business or proposed business; or***

(5) The lack of a market for your common equity securities or securities convertible into or exercisable for common equity securities.

(d) ***Ratio of earnings to fixed charges***. If you register debt securities, show a ratio of earnings to fixed charges. If you register preference equity securities, show the ratio of combined fixed charges and preference dividends to earnings. Present the ratio for each of the last five fiscal years and the latest interim period for which financial statements are presented in the document. If you will use the proceeds from the sale of debt or preference securities to repay any of your outstanding debt or to retire other securities and the change in the ratio would be ten percent or greater, you must include a ratio showing the application of the proceeds, commonly referred to as the pro forma ratio.

Instructions to paragraph 503(d): 1. *Definitions.* In calculating the ratio of earnings to fixed charges, you must use the following definitions:

(A) ***Fixed charges***. The term "fixed charges" means the sum of the following:

(a) interest expensed and capitalized, (b) amortized premiums, discounts and capitalized expenses related to indebtedness, (c) an estimate of the interest within rental expense, and (d) preference security dividend requirements of consolidated subsidiaries.

(B) ***Preference security dividend***. The term "preference security dividend" is the amount of pre-tax earnings that is required to pay the dividends on outstanding preference securities. The dividend requirement must be computed as the amount of the dividend divided by (1 minus the effective income tax rate applicable to continuing operations).

(C) ***Earnings***. The term "earnings" is the amount resulting from adding and subtracting the following items. Add the following:

(a) pre-tax income from continuing operations before adjustment for income or loss from equity investees; (b) fixed charges; (c) amortization of capitalized interest; (d) distributed income of equity investees; and (e) your share of pre-tax losses of equity investees for which charges arising from guarantees are included in fixed charges. From the total of the added items, subtract the following: (a) interest capitalized; (b) preference security dividend requirements of consolidated subsidiaries; and (c) the noncontrolling interest in pre-tax income of subsidiaries that have not incurred fixed charges. Equity investees are investments that you account for using the equity method of accounting. Public utilities following FASB ASC Topic 980, *Regulated Operations,* should not add amortization of capitalized interest in determining earnings, nor reduce fixed charges by any allowance for funds used during construction.

2. *Disclosure.* Disclose the following information when showing the ratio of earnings to fixed charges:

(A) ***Deficiency***. If a ratio indicates less than one-to-one coverage, disclose the dollar amount of the deficiency.

(B) ***Pro forma ratio***. You may show the pro forma ratio only for the most recent fiscal year and the latest interim period. Use the net change in interest or dividends from the refinancing to calculate the pro forma ratio.

(C) ***Foreign private issuers***. A foreign private issuer must show the ratio based on the figures in the primary financial statement. A foreign private issuer must show the ratio based on the figures resulting from the reconciliation to U.S. generally accepted accounting principles if this ratio is materially different.

(D) ***Summary Section***. If you provide a summary or similar section in the prospectus, show the ratios in that section.

3. *Exhibit.* File an exhibit to the registration statement to show the figures used to calculate the ratios. See paragraph (b)(12) of Item 601 of Regulation S-K (17 CFR 229.601(b)(12)).

(e) ***Smaller reporting companies***. A registrant that qualifies as a smaller reporting company, as defined by § 229.10(f), need not comply with paragraph (d) of this Item.

Instruction to Item 503*:* For asset-backed securities, see also Item 1103 of Regulation AB (§ 229.1103).

[63 FR 6383, Feb. 6, 1998, as amended at 70 FR 1594, Jan. 7, 2005; 73 FR 964, Jan. 4, 2008; 74 FR 18617, Apr. 23, 2009; 76 FR 50121, Aug. 12, 2011]

EXHIBIT C

Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus

Commissioner Luis A. Aguilar

"Cyber Risks and the Boardroom" Conference
New York Stock Exchange
New York, NY

June 10, 2014

Good afternoon. Thank you for that kind introduction. I am glad to be back at the New York Stock Exchange. In anticipating today's conference, I thought back to an earlier trip to the NYSE where in April 2009, I had the opportunity to ring the closing bell. Before I begin my remarks, let me issue the standard disclaimer that the views I express today are my own, and do not necessarily reflect the views of the U.S. Securities and Exchange Commission ("SEC" or "Commission"), my fellow Commissioners, or members of the staff.

I am pleased to be here and to have the opportunity to speak about cyber-risks and the boardroom, a topic that is both timely and extremely important. Over just a relatively short period of time, cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators.[1] I suspect that not too long ago, we would have been hard-pressed to find many individuals who had even heard of cybersecurity, let alone known what it meant. Yet, in the past few years, there can be no doubt that the focus on this issue has dramatically increased.[2]

Cybersecurity has become an important topic in both the private and public sectors, and for good reason. Law enforcement and financial regulators have stated publicly that cyber-attacks are becoming both more frequent and more sophisticated.[3] Indeed, according to one survey, U.S. companies experienced a 42% increase between 2011 and 2012 in the number of successful cyber-attacks they experienced per week.[4] As I am sure you have heard, recently there have also been a series of well-publicized cyber-attacks that have generated considerable media attention and raised public awareness of this issue. A few of the more well-known examples include:

- The October 2013 cyber-attack on the software company Adobe Systems, Inc., in which data from more than 38 million customer accounts was obtained improperly;[5]
- The December 2013 cyber-attack on Target Corporation, in which the payment card data of approximately 40 million Target customers and the personal data of up to 70 million Target customers was accessed without authorization;[6]
- The January 2014 cyber-attack on Snapchat, a mobile messaging service, in which a reported 4.6 million user names and phone numbers were exposed;[7]
- The sustained and repeated cyber-attacks against several large U.S. banks, in which their public websites have been knocked offline for hours at a time;[8] and
- The numerous cyber-attacks on the infrastructure underlying the capital markets, including quite a few on securities exchanges.[9]

In addition to becoming more frequent, there are reports indicating that cyber-attacks have become increasingly costly to companies that are attacked. According to one 2013 survey, the average annualized cost of cyber-crime to a sample of U.S. companies was $11.6 million per year, representing a 78% increase since 2009.[10] In addition, the aftermath of the 2013 Target data breach demonstrates that the impact of cyber-attacks may extend far beyond the direct costs associated with the immediate response to an attack.[11] Beyond the unacceptable damage to consumers, these secondary effects include reputational harm that significantly affects a company's bottom line. In sum, the capital markets and their critical participants, including public companies, are under a continuous and serious threat of cyber-attack, and this threat cannot be ignored.[12]

As an SEC Commissioner, the threats are a particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on public companies and investors.[13] The concern is not new. For example, in 2011, staff in the SEC's Division of Corporation Finance issued guidance to public companies regarding their disclosure obligations with respect to cybersecurity risks and cyber-incidents.[14] More recently, because of the escalation of cyber-attacks, I helped organize the Commission's March 26, 2014 roundtable to discuss the cyber-risks facing public companies and critical market participants like exchanges, broker-dealers, and transfer agents.[15]

Today, I would like to focus my remarks on what boards of directors can, and should, do to ensure that their organizations are appropriately considering and addressing cyber-risks. Effective board oversight of management's efforts to address these issues is critical to preventing and effectively responding to successful cyber-attacks and, ultimately, to protecting companies and their consumers, as well as protecting investors and the integrity of the capital markets.

The Role of the Boards of Directors in Overseeing Cyber-Risk Management

Background on the Role of Boards of Directors

When considering the board's role in addressing cybersecurity issues, it is useful to keep in mind the broad duties that the board owes to the corporation and, more specifically, the board's role in corporate governance and overseeing risk management. It has long been the accepted model, both here and around the world, that corporations are managed under the direction of their boards of directors.[16] This model arises from a central tenet of the modern corporation — the separation of ownership and control of the corporation. Under this structure, those who manage a corporation must answer to the true owners of the company — the shareholders.

It would be neither possible nor desirable, however, for the many, widely-dispersed shareholders of any public company to come together and manage, or direct the management of, that company's business and affairs. Clearly, effective full-time management is essential for public companies to function. But management without accountability can lead to self-interested decision-making that may not benefit the company or its shareholders. As a result, shareholders elect a board of directors to represent their interests, and, in turn, the board of directors, through effective corporate governance, makes sure that management effectively serves the corporation and its shareholders.[17]

Corporate Boards and Risk Management Generally

Although boards have long been responsible for overseeing multiple aspects of management's activities, since the financial crisis, there has been an increased focus on what boards of directors are doing to address risk management.[18] Indeed, many have noted that, leading up to the financial crisis, boards of directors may not have been doing enough to oversee risk management within their companies, and that this failure contributed to the unreasonably risky behavior that resulted in the destruction of untold billions in shareholder value and plunged the country and the global economy into recession.[19] Although primary responsibility for risk management has historically belonged to management, the boards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs.[20]

The importance of this oversight was highlighted when, in 2009, the Commission amended its rules to require disclosure about, among other things, the board's role in risk oversight, including a description of whether and how the board administers its oversight function, such as through the whole board, a separate risk committee, or the audit committee.[21] The Commission did not mandate any particular structure, but noted that "risk oversight is a key competence of the board" and that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[22]

The evidence suggests that boards of directors have begun to assume greater responsibility for overseeing the risk management efforts of their companies.[23] For example, according to a recent survey of 2013 proxy filings by companies comprising the S&P 200, the full boards of these companies are increasingly, and nearly universally, taking responsibility for the risk oversight of the company.[24]

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk[25] — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.[26]

What Boards of Directors Can and Should Be Doing to Oversee Cyber-Risk

Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant

threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. [27]

In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats.[28] Perhaps unsurprisingly, there has recently been a series of derivative lawsuits brought against companies and their officers and directors relating to data breaches resulting from cyber-attacks.[29] Thus, boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.

Given the known risks posed by cyber-attacks, one would expect that corporate boards and senior management universally would be proactively taking steps to confront these cyber-risks. Yet, evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks. Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues.[30] According to one survey, boards were not undertaking key oversight activities related to cyber-risks, such as reviewing annual budgets for privacy and IT security programs, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks.[31] Even when boards do pay attention to these risks, some have questioned the extent to which boards rely too much on the very personnel who implement those measures.[32] In light of these observations, directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management.

NIST Cybersecurity Framework

In considering where to begin to assess a company's possible cybersecurity measures, one conceptual roadmap boards should consider is the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology ("NIST") in February 2014. The NIST Cybersecurity Framework is intended to provide companies with a set of industry standards and best practices for managing their cybersecurity risks.[33] In essence, the Framework encourages companies to be proactive and to think about these difficult issues in advance of the occurrence of a possibly devastating cyber-event. While the Framework is voluntary guidance for any company, some commentators have already suggested that it will likely become a baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes.[34] At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed.

Board Structural Changes to Focus on Appropriate Cyber-Risk Management

The NIST Cybersecurity Framework, however, is a bible without a preacher if there is no one at the company who is able to translate its concepts into action plans. Frequently, the board's risk oversight function lies either with the full board or is delegated to the board's audit committee. Unfortunately, many boards lack the technical expertise necessary to be able to evaluate whether management is taking appropriate steps to address cybersecurity issues. Moreover, the board's audit committee may not have the expertise, support, or skills necessary to add oversight of a company's cyber-risk management to their already full agenda.[35] As a result, some have recommended mandatory cyber-risk education for directors.[36] Others have suggested that boards be at least adequately represented by members with a good understanding of information technology issues that pose risks to the company.[37]

Another way that has been identified to help curtail the knowledge gap and focus director attention on known cyber-risks is to create a separate enterprise risk committee on the board. It is believed that such committees can foster a "big picture" approach to company-wide risk that not only may result in improved risk reporting and monitoring for both management and the board, but also can provide a greater focus — at the board level — on the adequacy of resources and overall support provided to company executives responsible for risk management.[38] The Dodd-Frank Act already requires large financial institutions to establish independent risk committees on their boards.[39] Beyond the financial institutions required to do so, some public companies have chosen to proactively create such risk committees on their boards.[40] Research suggests that 48% of corporations currently have board-level risk committees that are responsible for privacy and security risks, which represents a dramatic increase from the 8% that reported having such a committee in 2008.[41]

Clearly, there are various mechanisms that boards can employ to close the gap in addressing cybersecurity concerns — but it is equally clear that boards need to be proactive in doing so. Put simply, boards that lack an adequate understanding of cyber-risks are unlikely to be able to effectively oversee cyber-risk management.

I commend the boards that are proactively addressing these new risks of the 21st Century. However, while enhancing board knowledge and board involvement is a good business practice, it is not necessarily a panacea to comprehensive cybersecurity oversight.

Internal Roles and Responsibilities Focused on Cyber-Risk

In addition to proactive boards, a company must also have the appropriate personnel to carry out effective cyber-risk management and to provide regular reports to the board. One 2012 survey reported that less than two-thirds of responding companies had full-time personnel in key roles responsible for privacy and security, in a manner that was consistent with internationally accepted best practices and standards.[42] In addition, a 2013 survey found that the companies that detected more security incidents and reported lower average financial losses per incident shared key attributes, including that they employed a full-time chief information security officer (or equivalent) who reported directly to senior management.[43]

At a minimum, boards should have a clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber-risk management practices.[44] In addition, as the evidence shows, devoting full-time personnel to cybersecurity issues may help prevent and mitigate the effects of cyber-attacks.

Board Preparedness

Although different companies may choose different paths, ultimately, the goal is the same: to prepare the company for the inevitable cyber-attack and the resulting fallout from such an event. As it has been noted, the primary distinction between a cyber-attack and other crises that a company may face is the speed with which the company must respond to contain the rapid spread of damage.[45] Companies need to be prepared to respond within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event.[46]

While there is no "one-size-fits-all" way to properly prepare for the various ways a cyber-attack can unfold, and what responses may be appropriate, it can be just as damaging to have a poorly-implemented response to a cyber-event. As others have observed, an "ill-thought-out response can be far more damaging than the attack itself."[47] Accordingly, boards should put time and resources into making sure that management has developed a well-constructed and deliberate response plan that is consistent with best practices for a company in the same

industry.

These plans should include, among other things, whether, and how, the cyber-attack will need to be disclosed internally and externally (both to customers and to investors).[48] In deciding the nature and extent of the disclosures, I would encourage companies to go beyond the impact on the company and to also consider the impact on others. It is possible that a cyber-attack may not have a direct material adverse impact on the company itself, but that a loss of customers' personal and financial data could have devastating effects on the lives of the company's customers and many Americans. In such cases, the right thing to do is to give these victims a heads-up so that they can protect themselves.[49]

Conclusion

Let me conclude my remarks by reaffirming the significance of the role of good corporate governance. Corporate governance performed properly, results in the protection of shareholder assets. Fortunately, many boards take on this difficult and challenging role and perform it well. They do so by, among other things, being active, informed, independent, involved, and focused on the interests of shareholders.

Good boards also recognize the need to adapt to new circumstances — such as the increasing risks of cyber-attacks. To that end, board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks.

Those of you who have taken the time and effort to be here today clearly recognize the risks, and I commend you for being proactive in dealing with the issue.

Thank you for inviting me to speak to you today.

---

[1] For example, the Director of the Federal Bureau of Investigation (FBI), James Comey, said last November that "resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats." *See,* Testimony of James B. Comey, Jr., Director, FBI, U.S. Department of Justice, before the Senate Committee on Homeland Security and Governmental Affairs (Nov. 14, 2013), *available at* http://www.hsgac.senate.gov/hearings/threats-to-the-homeland. *See also,* Testimony of Jeh C. Johnson, Secretary, U.S. Department of Homeland Security, before the House Committee on Homeland Security (Feb. 26, 2014) ("DHS must continue efforts to address the growing cyber threat to the private sector and the '.gov' networks, illustrated by the real, pervasive, and ongoing series of attacks on public and private infrastructure."), *available at* http://docs.house.gov/meetings/HM/HM00/20140226/101722/HHRG-113-HM00-Wstate-JohnsonJ-20140226.pdf; Testimony of Ari Baranoff, Assistant Special Agent in Charge, United States Secret Service Criminal Investigative Division, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies (Apr. 16, 2014), *available at* http://docs.house.gov/meetings/HM/HM08/20140416/102141/HHRG-113-HM08-Wstate-BaranoffA-20140416.pdf ("Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cybercrimes

targeting private industry and critical infrastructure."); Remarks by Secretary of Defense Leon E. Panetta to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("As director of the CIA and now Secretary of Defense, I have understood that cyber attacks are every bit as real as the more well-known threats like terrorism, nuclear weapons proliferation and the turmoil that we see in the Middle East. And the cyber threats facing this country are growing.").

[2] *See, e.g.*, Martin Lipton, *et al.*, *Risk Management and the Board of Directors — An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Apr. 22, 2014), *available at* http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014/ (noting that cybersecurity is a risk management issue that "merits special attention" from the board of directors in 2014); PwC 2012 Annual Corporate Directors Survey, *Insights from the Boardroom 2012: Board evolution: Progress made yet challenges persist*, *available at* http://www.pwc.com/en_US/us/corporate-governance/annual-corporate-directors-survey/assets/pdf/pwc-annual-corporate-directors-survey.pdf (finding that 72% of directors are engaged with overseeing and understanding data security issues and risks related to compromising customer data); Michael A. Gold, *Cyber Risk and the Board of Directors–Closing the Gap*, Bloomberg BNA (Oct. 18, 2013) *available at* http://www.bna.com/cyber-risk-and-the-board-of-directors-closing-the-gap// ("The responsibility of corporate directors to address cyber security is commanding more attention and is obviously a significant issue."); Deloitte Development LLC, *Hot Topics: Cybersecurity … Continued in the boardroom*, Corporate Governance Monthly (Aug. 2013), *available at* http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/USEng/Documents/Deloitte%20Periodicals/Hot%20Topics/Hot%20Topics%20-%20Cybersecurity%20%20%20Continued%20in%20the%20boardroom%20-August%202013%20-Final.pdf ("Not long ago, the term 'cybersecurity' was not frequently heard or addressed in the boardroom. Cybersecurity was often referred to as an information technology risk, and management and oversight were the responsibility of the chief information or technology officer, not the board. With the rapid advancement of technology, cybersecurity has become an increasingly challenging risk that boards may need to address."); Holly J. Gregory, *Board Oversight of Cybersecurity Risks*, Thomson Reuters Practical Law (Mar. 1, 2014), *available at* http://us.practicallaw.com/5-558-2825 ("The risk of cybersecurity breaches (and the harm that these breaches pose) is one of increasing significance for most companies and therefore an area for heightened board focus.").

[3] For example, on December 9, 2013, the Financial Stability Oversight Council held a meeting to discuss cybersecurity threats to the financial system. *See*, U.S. Department of the Treasury Press Release, "Financial Stability Oversight Council to Meet December 9," *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2228.aspx. During that meeting, Assistant Treasury Secretary Cyrus-Amir-Mokri said that "[o]ur experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication." *See,* Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council (Dec. 9, 2013), *available at* http://www.treasury.gov/press-center/press-releases/Pages/jl2234.aspx. In addition, in testimony before the House Financial Services Committee in 2011, the Assistant Director of the FBI's Cyber Division stated that the number and sophistication of malicious incidents involving financial institutions has increased dramatically over the past several years and offered numerous examples of such attacks, which included fraudulent monetary transfers, unauthorized financial transactions from compromised bank and brokerage accounts, denial of service attacks on U.S. stock exchanges, and hacking incidents in which confidential information was misappropriated. *See,* Testimony of Gordon M. Snow, Assistant Director, Cyber Division, FBI, U.S. Department of Justice, before the House Financial Services Committee,

Subcommittee on Financial Institutions and Consumer Credit (Sept. 14, 2011), *available at* http://financialservices.house.gov/uploadedfiles/091411snow.pdf.

[4] *2012 Cost of Cyber Crime Study: United States*, Ponemon Institute LLC and HP Enterprise Security (Oct. 2012), *available at* http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf.

[5] *See, e.g.,* Jim Finkle, *Adobe says customer data, source code accessed in cyber attack*, Reuters (Oct. 3, 2013), *available at* http://www.reuters.com/article/2013/10/03/us-adobe-cyberattack-idUSBRE99212Y20131003; Jim Finkle, *Adobe data breach more extensive than previously disclosed*, Reuters (Oct. 29, 2013), *available at* http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029; Danny Yadron, *Hacker Attack on Adobe Sends Ripples Across Web*, Wall Street Journal (Nov. 11, 2013), *available at* http://online.wsj.com/news/articles/SB10001424052702304644104579192393329283358.

[6] *See,* Testimony of John Mulligan, Executive Vice President and Chief Financial Officer of Target, before the Senate Judiciary Committee (Feb. 4, 2014), *available at* http://www.judiciary.senate.gov/imo/media/doc/02-04-14MulliganTestimony.pdf ; Target Press Release, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores" (Dec. 19, 2013), *available at* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.

[7] *See, e.g.,* Andrea Chang and Salvador Rodriguez, *Snapchat becomes target of widespread cyberattack*, L.A. Times (Jan. 2, 2014), *available at* http://articles.latimes.com/2014/jan/02/business/la-fi-snapchat-hack-20140103; Brian Fung, *A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix?* Washington Post (Jan. 1, 2014), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/.

[8] *See, e.g.,* Joseph Menn, *Cyber attacks against banks more severe than most realize*, Reuters (May 18, 2013), *available at* http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518; Bob Sullivan, *Bank Website Attacks Reach New Highs*, CNBC (Apr. 3, 2013), *available at* http://www.cnbc.com/id/100613270.

[9] For example, according to a 2012 global survey of securities exchanges, 53% reported experiencing a cyber-attack in the previous year. *See,* Rohini Tendulkar, *Cyber-crime, securities markets, and systemic risk*, Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges (July 16, 2013), *available at* http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf. Forty-six securities exchanges responded to the survey.

[10] *See*, HP Press Release, *HP Reveals Cost of Cybercrime Escalates 70 Percent, Time to Resolve Attacks More Than Doubles* (Oct. 8, 2013), *available at* http://www8.hp.com/us/en/hp-news/press-release.html?id=1501128.

[11] *See*, Target Financial News Release, *Target Reports Fourth Quarter and Full-Year 2013 Earnings* (Feb. 26, 2014), *available at* http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight (including a statement from then-Chairman, President and CEO Gregg Steinhafel that Target's fourth quarter results "softened meaningfully following our December announcement of a data breach."); Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. Times (Feb. 26, 2014), *available at* http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?

_r=0 (noting that "[t]he widespread theft of Target customer data had a significant impact on the company's profit, which fell more than 40 percent in the fourth quarter" of 2013).

[12] I also want to note that at the Investment Company Institute's ("ICI") general membership meeting, held just last month, the issue of cybersecurity was front and center. Among the issues raised during the meeting was the "huge risk to brand" for a firm if they have a security failure in the event of a cyber-attack. A separate panel at the ICI conference devoted to cybersecurity also discussed the shift in focus from building "hard walls" to protect against risks from outside the company to cybersecurity focused on "inside" risks, such as ensuring that individuals with mobile applications or other types of flexible applications don't introduce, intentionally or unintentionally, malware or other kinds of security breaches that could lead to a cyber-attack on the company. *See, e.g.,* Jackie Noblett, *Cyber Breach a "Huge Risk to Brand,"* Ignites (May 29, 2014), *available at* http://ignites.com/c/897654/86334/cyber_breach_huge_risk_brand?referrer_module=emailMorningNews&module_order=7.

[13] *See,* Commissioner Luis A. Aguilar, *The Commission's Role in Addressing the Growing Cyber-Threat* (Mar. 26, 2014), *available at* http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.

[14] On October 13, 2011, staff in the Commission's Division of Corporation Finance (Corp Fin) issued guidance on issuers' disclosure obligations relating to cyber security risks and cyber incidents. *See,* SEC's Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2—Cybersecurity* ("SEC Guidance") (Oct. 31, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Among other things, this guidance notes that securities laws are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision, and cybersecurity risks and events are not exempt from these requirements. The guidance identifies six areas where cybersecurity disclosures may be necessary under Regulation S-K: (1) Risk Factors; (2) Management's Discussion and Analysis of Financial Condition and Results of Operation (MD&A); (3) Description of Business; (4) Legal Proceedings; (5) Financial Statement Disclosures; and (6) Disclosure Controls and Procedures. The SEC Guidance further recommends that material cybersecurity risks should be disclosed and adequately described as Risk Factors. Where cybersecurity risks and incidents that represent a material event, trend or uncertainty reasonably likely to have a material impact on the organization's operations, liquidity, or financial condition — it should be addressed in the MD&A. If cybersecurity risks materially affect the organization's products, services, relationships with customers or suppliers, or competitive conditions, the organization should disclose such risks in its description of business. Data breaches or other incidents can result in regulatory investigations or private actions that are material and should be discussed in the Legal Proceedings section. Cybersecurity risks and incidents that represent substantial costs in prevention or response should be included in Financial Statement Disclosures where the financial impact is material. Finally, where a cybersecurity risk or incident impairs the organization's ability to record or report information that must be disclosed, Disclosure Controls and Procedures that fail to address cybersecurity concerns may be ineffective and subject to disclosure. Some have suggested that such disclosures fail to fully inform investors about the true costs and benefits of companies' cybersecurity practices, and argue that the Commission (and not the staff) should issue further guidance regarding issuers' disclosure obligations. *See,* Letter from U.S. Senator John D. Rockefeller IV to Chair White (Apr. 9, 2013), *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51.

[15] *See* SEC Press Release, *SEC Announces Agenda, Panelists for Cybersecurity Roundtable* (Mar. 24, 2014), *available at*

http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541253749; *Cybersecurity Roundtable Webcast* (Mar. 26, 2014), *available at* http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml. In addition, the SEC's National Exam Program has included cybersecurity among its areas of focus in its National Examination Priorities for 2014. *See,* SEC's National Exam Priorities for 2014, *available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf. In addition, it was recently announced that SEC examiners will review whether asset managers have policies to prevent and detect cyber-attacks and are properly safeguarding against security risks that could arise from vendors having access to their systems. *See,* Sarah N. Lynch, *SEC examiners to review how asset managers fend off cyber attacks*, Reuters (Jan. 30, 2014), *available at* http://www.reuters.com/article/2014/01/30/us-sec-cyber-assetmanagers-idUSBREA0T1PJ20140130. FINRA has also identified cybersecurity as one of its examination priorities for 2014. *See,* FINRA's 2014 Regulatory and Examination Priorities Letter (Jan. 2, 2014), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p419710.pdf.

To continue the discussion and to allow the public to weigh in on this important topic, the SEC set up a public comment file associated with the Cybersecurity Roundtable. To date, we have received ten comment letters from academics, software companies, and other interested parties, *available at* http://www.sec.gov/comments/4-673/4-673.shtml. *See, e.g.*, Jodie Kelly, Senior Vice President and General Counsel, BSA| The Software Alliance comment letter (Apr. 30, 2014) (highlighting the importance of strong internal controls related to software assets as a first line of defense against cyber-attacks, and noting that verifying legal use of software is a critical first step in deterring cyber-attacks because the "existence and availability of pirated and counterfeit software exposes corporate information technology networks to significant risks in many ways."); Tom C.W. Lin, Associate Professor of Law, Temple University Beasley School of Law comment letter (Apr. 29, 2014) (expressing support for the roundtable and the Commission's attention to cybersecurity and highlighting four broad issues for the Commission's consideration: (1) cybersecurity threats to the high-speed, electronically connected modern capital markets can create systemic risks; (2) due to technological advances, financial choices are made by both people and machines, which does not comport congruently with many traditional modes of securities regulation; (3) incentives, in addition to penalties, should be designed to encourage firms to upgrade their cybersecurity capabilities; and (4) private regulation of cybersecurity should be vigorously enhanced and leveraged to better complement government regulation); Dave Parsonage, CEO, MitoSystems, Inc. comment letter (Apr. 3, 2014); Gail P. Ricketts, Senior IT Compliance and Risk Analyst, ON Semiconductor comment letter (Mar. 26, 2014) (suggesting future roundtables include speakers from outside the financial services industry, such as manufacturing); Michael Utzig, IT Director, Hefren Tillotson, Inc. comment letter (Mar. 26, 2014) (noting that readily available technologies that can protect email communications are not widely used despite universal understanding that cybersecurity is a high-priority); Cathy Santoro comment letter (Mar. 26, 2014) (raising questions about the interactions between banks and service providers and the measures being undertaken regarding mobile payment cybersecurity risks); Duane Kuroda, Senior Threat Researcher, NetCitadel comment letter (Mar. 25, 2014) (noting that the panel discussion should focus on the process and people involved in responding to breaches and not just their detection); William Pfister, Jr. comment letter (Mar. 25, 2014) (requesting that one of the panels address the potential conflicts between national security and required disclosure). Many of these letters are generally supportive of the Commission's efforts and focus in this area, and some identify issues and concerns that were not discussed in detail during the roundtable and warrant further attention. For example, one commenter highlighted the need for companies to adopt sound internal controls over the legal use of software, noting that pirated and counterfeit software can

expose companies to heightened risk of cyber-attacks and recommending that registrants report on the status of such internal controls.[15] *See, e.g.*, Jodie Kelly, Senior Vice President and General Counsel, BSA| The Software Alliance comment letter (Apr. 30, 2014) (noting, among other things, that unlicensed software eliminates the opportunity for security updates and patches from legitimate vendors when security breaches are identified, and that malware and viruses may be contained within pirated software itself or reside on the networks from which it is downloaded. BSA recommends that registrants report on the status of their internal controls in the area of licensing and legal use of software, and that such controls should, at a minimum, ensure that software is only purchased from authorized vendors and that companies should have procedures to conduct periodic software inventories and limit exposure to malware and viruses brought into their systems by linkage of employees' personal devices to corporate systems). I encourage others to comment and provide valuable input on this critical issue.

[16] *See, e.g.*, Model Bus. Corp. Act § 8.01 (2002); Del. Gen. Corp. Law § 141(a).

[17] For additional thoughts on the importance of effective corporate governance, *see* Commissioner Luis A. Aguilar, *Looking at Corporate Governance from the Investor's Perspective*, *available at* http://www.sec.gov/News/Speech/Detail/Speech/1370541547078.

[18] *See, e.g.*, Committee of Sponsoring Organizations of the Treadway Commission, *Effective Enterprise Risk Oversight: The Role of the Board of Directors* (2009), *available at* http://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf ("Clearly, one result of the financial crisis is an increased focus on the effectiveness of board risk oversight practices."); Committee of Sponsoring Organizations of the Treadway Commission, *Board Risk Oversight: A Progress Report — Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities* (Dec. 2010), *available at* http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf ("Risk oversight is a high priority on the agenda of most boards of directors. Recently, the importance of this responsibility has become more evident in the wake of an historic global financial crisis, which disclosed perceived risk management weaknesses across financial services and other organizations worldwide. Based on numerous legislative and regulatory actions in the United States and other countries as well as initiatives in the private sector, it is clear that expectations for more effective risk oversight are being raised not just for financial services companies, but broadly across all types of businesses."); David A. Katz, *Boards Play A Leading Role in Risk Management Oversight*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Oct. 8, 2009), *available at* http://blogs.law.harvard.edu/corpgov/2009/10/08/boards-play-a-leading-role-in-risk-management-oversight/ ("Just as the Enron and other high-profile corporate scandals were seen as resulting from a lack of ethics and oversight, the credit market meltdown and resulting financial crisis have been blamed in large part on inadequate risk management by corporations and their boards of directors. As a result, along with the task of implementing corporate governance procedures and guidelines, a company's board of directors is expected to take a leading role in overseeing risk management structures and policies.").

[19] Nicola Faith Sharpe, *Informational Autonomy in the Boardroom*, 201 U. Ill. L. Rev. 1089 (2013) ("The financial crisis of 2007-2008 was one of the worst in U.S. history. In a single quarter, the blue chip company Lehman Brothers (who eventually went bankrupt) lost $2.8 billion. While commentators have identified multiple reasons why the crisis occurred, many posit that boards mismanaged risk and failed in their oversight duties, which directly contributed to their firms failing."); Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. Marshall J. Computer & Info. L. 313 (Spring 2011) ("With accusations that boards of directors of financial institutions were asleep at the wheel while their companies engaged in risky behavior that erased millions of

dollars of shareholder value and plunged the country into recession, increasing pressure is now being placed on public company boards to shoulder the burden of risk oversight for the companies they serve."); William B. Asher, Jr., Michael T. Gass, Erik Skramstad, and Michele Edwards, *The Role of Board of Directors in Risk Oversight in a Post-Crisis Economy*, Bloomberg Law Reports-Corporate Law Vol. 4, No. 13, *available at* http://www.choate.com/uploads/113/doc/Asher,%20Gass%20-The%20Role%20of%20Board%20of%20Directors%20in%20Risk%20Oversight%20in%20a%20Post-Crisis%20Economy.pdf ("Senior management and corporate directors face renewed criticism surrounding risk management practices and apparent failures in oversight that are considered, at least in part, to be at the root of the recent crisis.").

[20] *See, e.g.,* Stephen M. Bainbridge, *Caremark and Enterprise Risk Management*, 34 Iowa J. Corp. L. 967 (2009) ("Although primary responsibility for risk management rests with the corporation's top management team, the board of directors is responsible for ensuring that the corporation has established appropriate risk management programs and for overseeing management's implementation of such programs."); Martin Lipton, *Risk Management and the Board of Directors–An Update for 2014*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Apr. 22, 2014), *available at* http://blogs.law.harvard.edu/corpgov/2014/04/22/risk-management-and-the-board-of-directors-an-update-for-2014/ (". . . the board cannot and should not be involved in actual day-to day risk *management*. Directors should instead, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, the board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is instead an integral component of strategy, culture and business operations.").

[21] *Proxy Disclosure Enhancements*, SEC Rel. No. 33-9089 (Dec. 16, 2009), 74 Fed. Reg. 68334, *available at* http://www.sec.gov/rules/final/2009/33-9089.pdf.

[22] *Id.* That amendment also required disclosure of a company's compensation policies and practices as they relate to a company's risk management in order to help investors identify whether the company has established a system of incentives that could lead to excessive or inappropriate risk taking by its employees.

[23] *Supra* note 19, William B. Asher, Jr. *et al.*, *The Role of Board of Directors in Risk Oversight in a Post-Crisis Economy* ("We know today, however, that risk management has indeed forced its way into the boardroom and that there has been a substantial change in the relationship between the overseers of public companies and their shareholders.").

[24] *Risk Intelligent Proxy Disclosures — 2013: Trending upward*, Deloitte (2013), *available at* http://deloitte.wsj.com/riskandcompliance/files/2014/01/Risk_Intelligent_Proxy_Disclosures_2013.pdf (noting that 91% of the issuers of proxy disclosures noted that "the full board is responsible for risk.").

[25] See, *Proxy Disclosure Enhancements*, *supra* note 21.

[26] Paul Ziobro, *Target Shareholders Should Oust Directors, ISS Says*, Wall St. Journal (May

28, 2014), *available at* http://online.wsj.com/article/BT-CO-20140528-709863.html; Bruce Carton, *ISS Recommends Ouster of Seven Target Directors for Data Breach Failures*, ComplianceWeek (May 29, 2014), *available at* http://www.complianceweek.com/iss-recommends-ouster-of-seven-target-directors-for-data-breach-failures/article/348954/?DCMP=EMC-CW-WeekendEdition.

[27] *See, e.g.*, *Risk Management and the Board of Directors–An Update for* 2014, *supra* note 2 (noting that cybersecurity is a risk management issue that "merits special attention" from the board of directors in 2014); Alice Hsu, Tracy Crum, Francine E. Friedman, and Karol A. Kepchar, *Cybersecurity Update: Are Data Breach Disclosure Requirements On Target?*, The Metropolitan Corporate Counsel (Jan. 24, 2014), *available at* http://www.metrocorpcounsel.com/articles/27148/cybersecurity-update-are-data-breach-disclosure-requirements-target ("As part of a board's risk management oversight function, directors should assess the adequacy of their company's data security measures. Among other things, boards should have a clear understanding of the company's cybersecurity risk profile and who has primary responsibility for cybersecurity risk oversight and should ensure the adequacy of the company's cyber risk management practices, as well as the company's insurance coverage for losses and costs associate with data breaches.").

[28] Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 Rich. J.L. & Tech. 12 (2013), *available at* http://jolt.richmond.edu/v19i4/article12.pdf. (indicating that "[t]he principles thus enunciated raise the specter of potential liability if officers and directors utterly fail to ensure the adequacy of information systems."); J. Wylie Donald and Jennifer Black Strutt, *Cybersecurity: Moving Toward a Standard of Care for the Board,* Bloomberg BNA (Nov. 4, 2013), *available at* http://www.bna.com/cybersecurity-moving-toward-a-standard-of-care-for-the-board/ (quoting from a Delaware Chancery Court decision stating that directors may be liable if "(a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.").

[29] *See, e.g., Collier v. Steinhafel et al.* (D.C. Minn. Jan. 2014), case number 0:14-cv-00266 (alleging that Target's board and top executives harmed the company financially by failing to take adequate steps to prevent the cyber-attack then by subsequently providing customers with misleading information about the extent of the data theft.); *Dennis Palkon et al. v. Stephen P. Holmes et al*. (D.C.N.J. May 2014), case number 2:14-cv-01234 (alleging that Wyndham's board and top executives harmed the company financially by failing to take adequate steps to safeguard customers' personal and financial information.).

[30] Steven P. Blonder, *How closely is the board paying attention to cyber risks?*, Inside Counsel (formerly Corporate Legal Times) (Apr. 9, 2014), *available at* http://www.insidecounsel.com/2014/04/09/how-closely-is-the-board-paying-attention-to-cyber. (Indicating that "[i]n all likelihood, absent an incident, it is likely that board members are not spending sufficient time evaluating or analyzing the risks inherent in new technologies, as well as their related cybersecurity risks.").

[31] Jody R. Westby, *Governance of Enterprise Security: CyLab 2012 Report — How Boards & Senior Executives Are Managing Cyber Risks*, Carnegie Mellon University CyLab (May 16, 2012), at 5. (Hereinafter "CyLab 2012 Report.").

[32] *Supra note 30,* Steven P. Blonder, *How Closely is the Board Paying Attention to Cyber Risks?* (stating that "[f]urther, even if a board has evaluated these risks, to what extent is such an evaluation dependent on a company's IT department — the same group implementing the existing technology protocols?").

[33] The National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) (the "NIST Cybersecurity Framework"), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, was released in response to President Obama's issued Executive Order 13636, titled "Improving Critical Infrastructure Cybersecuity," dated February 12, 2013. The NIST Cybersecurity Framework sets out five core functions and categories of activities for companies to implement that relate generally to cyber-risk management and oversight, which the NIST helpfully boiled down to five terms: Identify, Protect, Detect, Respond and Recover. This core fundamentally means the following: companies should (i) *identify* known cybersecurity risks to their infrastructure; (ii) develop safeguards to *protect* the delivery and maintenance of infrastructure services; (iii) implement methods to *detect* the occurrence of a cybersecurity event; (iv) develop methods to *respond* to a detected cybersecurity event; and (v) develop plans to *recover* and restore the companies' capabilities that were impaired as a result of a cybersecurity event. *See also,* Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*, The Metropolitan Corporate Counsel (Mar. 17, 2014), *available at* http://www.sheppardmullin.com/media/article/1280_MCC-Cybersecurity-Breaching%20The%20Boardroom.pdf.

[34] *Supra note* 2*,* Holly J. Gregory, *Board Oversight of Cybersecurity Risks; supra note* 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom* (stating that "[w]hile adoption of the Cybersecurity Framework is voluntary, it will likely become a key reference for regulators, insurance companies and the plaintiffs' bar in assessing whether a company took steps reasonably designed to reduce and manage cybersecurity risks.").

[35] Matteo Tonello, *Should Your Board Have a Separate Risk Committee?*, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Feb. 12, 2012), *available at* https://blogs.law.harvard.edu/corpgov/2012/02/12/should-your-board-have-a-separate-risk-committee/ (asking "[d]oes the audit committee have the time, the skills, and the support to do the job, given everything else it is required to do?").

[36] *See, e.g.*, Katie W. Johnson, *Publicly Traded Companies Should Prepare To Disclose Cybersecurity Risks, Incidents*, Bloomberg BNA (Mar. 17, 2014), *available at* http://www.bna.com/publicly-traded-companies-n17179885721/ (citing Mary Ellen Callahan, Chair of the Privacy and Information Governance Practice at Jenner & Block, LLP at the International Association of Privacy Professionals Global Privacy Summit, held in March 2014); Michael A. Gold, *Cyber Risk and the Board of Directors — Closing the Gap*, Bloomberg BNA (Oct. 18, 2013), *available at* http://www.bna.com/cyber-risk-and-the-board-of-directors-closing-the-gap// (suggesting that companies would do well to have "[m]andatory cyber risk education for directors," among other things.); *see also, The Comprehensive National Cybersecurity Initiative*, initially launched by then-President George W. Bush in 2008, referencing "Initiative #8. Expand cyber education," and *available at* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[37] *Supra* note 19, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[38] *Supra* note 35, Matteo Tonello, *Should Your Board Have a Separate Risk Committee?*; *supra* note 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*.

[39] Dodd-Frank Act Section 165(h).

[40] *Supra* note 19, Lawrence J. Trautman and Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*.

[41] Deloitte Audit Committee Brief, *Cybersecurity and the audit committee* (Aug. 2013), at 2, *available at* http://deloitte.wsj.com/cfo/files/2013/08/ACBrief_August2013.pdf.

[42] *See*, *supra* note 31, CyLab 2012 Report, at 27.

[43] PricewaterhouseCoopers LLP, *The Global State of Information Security Survey 2014*, at 4, *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml (the "PwC IS Survey"). The PwC IS Survey also noted other shared attributes, such as having (i) an overall information security strategy; (ii) measured and reviewed the effectiveness of their security measures within the past year; and (iii) an understanding as to exactly what type of security events have occurred in the past year. *See also*, *supra* note 2, Holly Gregory, *Board Oversight of Cybersecurity Risks*.

[44] *Supra* note 27, Alice Hsu, *et al.*, *Cybersecurity Update: Are Data Breach Disclosure Requirements on Target?*.

[45] *See, e.g.,* Roland L. Trope and Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid,* 40 Wm. Mitchell L. Rev. 647 (2014), at 656 (stating that "unlike other corporate crises, boards and management must be ready to address severe cyber incidents with response and recovery plans that activate upon discovery of an intrusion and with little or no time for deliberation.") Some observers have even suggested that companies conduct "cyberwar games" organized around hypothetical business scenarios in order to reenact how a company might respond in a real cybersecurity situation in order to fix what vulnerabilities are teased out from the simulated scenario. Tucker Bailey, James Kaplan, and Allen Weinberg, *Playing war games to prepare for a cyberattack*, McKinsey & Company Insights & Publications (July 2012). Other observers have suggested that companies implement a response plan that takes into consideration a number of factors, such as (i) how much risk the company can accept if systems or services have to shut down; (ii) for how long the company can sustain operations using limited or backup technology; and (iii) how quickly the company can restore full operations. *See, Former FBI Agent Mary Galligan on Preparing for a Cyber Attack,* CIO Journal, Deloitte Insights (Mar. 3, 2104), *available at* http://deloitte.wsj.com/cio/2014/03/03/former-fbi-agent-mary-galligan-on-preparing-for-a-cyber-attack/.

[46] *See, e.g., id*., Roland L. Trope and Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, at 656.

[47] *Supra* note 45, Tucker Bailey, James Kaplan, and Allen Weinberg, *Playing War Games to Prepare for a Cyberattack*.

[48] *Supra* note 33, Ariel Yehezkel and Thomas Michael, *Cybersecurity: Breaching the Boardroom*, Metropolitan Corporate Counsel (stating that "Boards should prepare for worst-case scenario cybersecurity breaches and help management develop immediate response plans, including public disclosure procedures and economic recovery strategies, to mitigate potential damages." In addition, "[b]oards should consider disclosing cybersecurity risks and protective measures on relevant SEC filings, as such disclosures can generate confidence in investors rather than fear.") The U.S. Department of Commerce also has suggested that a company's cybersecurity preparedness could include cybersecurity insurance, which is specifically designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. *Cybersecurity Insurance*, U.S. Department of Homeland Security, *available at* http://www.dhs.gov/publication/cybersecurity-insurance. Despite the increased threats of cyber-attacks, the cybersecurity insurance market has been slow to develop, and many companies have chosen to forego available policies, citing their perceived high cost, a lack of awareness about what they cover, and their confidence (or ignorance) about

their actual risk of a cyber-attack. *Id.* Moreover, despite the fact that cyber incidents are not covered by general liability policies, one survey noted that 57% of respondents indicated that their boards are not reviewing their existing policies for cyber-related risks. *See*, *supra* note 31, CyLab 2012 Report, at 15.

[49] The Department of Justice recently unsealed indictments against five Chinese military officials who allegedly conspired to steal information from U.S. companies across different industries. In connection with this indictment, it was recently reported that three U.S. public companies identified as victims of this conspiracy failed to report the theft of trade secrets and other data to their investors, despite the Commission's disclosure guidance on this topic. Two of the companies, Alcoa Inc. and Allegheny Technologies Inc., said that the thefts were not "material," and therefore did not have to be disclosed to investors. *See,* Chris Strohm, Dave Michaels and Sonja Elmquist, *U.S. Companies Hacked by Chinese Didn't Tell Investors*, Bloomberg (May 21, 2014), *available at* http://www.bloomberg.com/news/2014-05-21/u-s-companies-hacked-by-chinese-didn-t-tell-investors.html*; See also, supra note 14.*

Modified: June 10, 2014

EXHIBIT D

101 S.Ct. 677
Supreme Court of the United States

UPJOHN COMPANY et al., Petitioners,
v.
UNITED STATES et al.

No. 79–886.
|
Argued Nov. 5, 1980.
|
Decided Jan. 13, 1981.

Corporation and in–house general counsel appealed from order of the United States District Court for the Western District of Michigan, Noel P. Fox, Chief Judge, enforcing an Internal Revenue summons for documents. The Court of Appeals, Sixth Circuit, 600 F.2d 1223, affirmed in part, reversed in part and remanded. Certiorari was granted, and the Supreme Court, Justice Rehnquist, held that: (1) District Court's test, of availability of attorney–client privilege, was objectionable as it restricted availability of privilege to those corporate officers who played "substantial role" in deciding and directing corporation's legal response; (2) where communications at issue were made by corporate employees to counsel for corporation acting as such, at direction of corporate superiors in order to secure legal advice from counsel, and employees were aware that they were being questioned so that corporation could obtain advice, such communications were protected; and (3) where notes and memoranda sought by government were work products based on oral statements of witnesses, they were, if they revealed communications, protected by privilege, and to extent they did not reveal communications, they revealed attorney's mental processes in evaluating the communications and disclosure would not be required simply on showing of substantial need and inability to obtain equivalent without undue hardship.

Judgment of Court of Appeals reversed, and case remanded.

Chief Justice Burger filed an opinion concurring in part and concurring in the judgment.

****679** *Syllabus* [*]

***383** When the General Counsel for petitioner pharmaceutical manufacturing corporation (hereafter petitioner) was informed that one of its foreign subsidiaries had made questionable payments to foreign government officials in order to secure government business, an internal investigation of such payments was initiated. As part of this investigation, petitioner's attorneys sent a questionnaire to all foreign managers seeking detailed information concerning such payments, and the responses were returned to the General Counsel. The General Counsel and outside counsel also interviewed the recipients of the questionnaire and other company officers and employees. Subsequently, based on a report voluntarily submitted by petitioner disclosing the questionable payments, the Internal Revenue Service (IRS) began an investigation to determine the tax consequences of such payments and issued a summons pursuant to 26 U.S.C. § 7602 demanding production of, *inter alia*, the questionnaires and the memoranda and notes of the interviews. Petitioner refused to produce the documents on the grounds that they were protected from disclosure by the attorney–client privilege and constituted the work product of attorneys prepared in anticipation of litigation. The United States then filed a petition in Federal District Court seeking enforcement of the summons. That court adopted the Magistrate's recommendation that the summons should be enforced, the Magistrate having concluded, *inter alia*, that the attorney–client privilege had been waived and that the Government had made a sufficient showing of necessity to overcome the protection of the work–product doctrine. The Court of Appeals rejected the Magistrate's finding of a waiver of the attorney–client privilege, but held that under the so–called "control group test" the privilege did not apply "[t]o the extent that the communications were made by officers and agents not responsible for directing [petitioner's] actions in response to legal advice ... for the simple reason that the communications were not the 'client's.' " The court also held that the work–product doctrine did not apply to IRS summonses.

Held:

1. The communications by petitioner's employees to counsel are covered by the attorney–client privilege insofar as the responses to the ***384** questionnaires and any notes reflecting responses to interview questions are concerned. Pp. 682–686.

(a) The control group test overlooks the fact that such privilege exists to protect not only the giving of professional

advice to ****680** those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice. While in the case of the individual client the provider of information and the person who acts on the lawyer's advice are one and the same, in the corporate context it will frequently be employees beyond the control group (as defined by the Court of Appeals) who will possess the information needed by the corporation's lawyers. Middle–level—and indeed lower–level—employees can, by actions within the scope of their employment, embroil the corporation in serious legal difficulties, and it is only natural that these employees would have the relevant information needed by corporate counsel if he is adequately to advise the client with respect to such actual or potential difficulties. Pp. 683–684.

(b) The control group test thus frustrates the very purpose of the attorney–client privilege by discouraging the communication of relevant information by employees of the client corporation to attorneys seeking to render legal advice to the client. The attorney's advice will also frequently be more significant to noncontrol employees than to those who officially sanction the advice, and the control group test makes it more difficult to convey full and frank legal advice to the employees who will put into effect the client corporation's policy. P. 684.

(c) The narrow scope given the attorney–client privilege by the Court of Appeals not only makes it difficult for corporate attorneys to formulate sound advice when their client is faced with a specific legal problem but also threatens to limit the valuable efforts of corporate counsel to ensure their client's compliance with the law. P. 684.

(d) Here, the communications at issue were made by petitioner's employees to counsel for petitioner acting as such, at the direction of corporate superiors in order to secure legal advice from counsel. Information not available from upper–echelon management was needed to supply a basis for legal advice concerning compliance with securities and tax laws, foreign laws, currency regulations, duties to shareholders, and potential litigation in each of these areas. The communications concerned matters within the scope of the employees' corporate duties, and the employees themselves were sufficiently aware that they were being questioned in order that the corporation could obtain legal advice. P. 685.

2. The work–product doctrine applies to IRS summonses. Pp. 686–689.

(a) The obligation imposed by a tax summons remains subject to the traditional privileges and limitations, and nothing in the language ***385** or legislative history of the IRS summons provisions suggests an intent on the part of Congress to preclude application of the work–product doctrine. P. 687.

(b) The Magistrate applied the wrong standard when he concluded that the Government had made a sufficient showing of necessity to overcome the protections of the work–product doctrine. The notes and memoranda sought by the Government constitute work product based on oral statements. If they reveal communications, they are protected by the attorney–client privilege. To the extent they do not reveal communications they reveal attorneys' mental processes in evaluating the communications. As Federal Rule of Civil Procedure 26, which accords special protection from disclosure to work product revealing an attorney's mental processes, and *Hickman v. Taylor*, 329 U.S. 495, 67 S.Ct. 385, 91 L.Ed. 451, make clear, such work product cannot be disclosed simply on a showing of substantial need or inability to obtain the equivalent without undue hardship. P. 688.

600 F.2d 1223, 6 Cir., reversed and remanded.

Attorneys and Law Firms

Daniel M. Gribbon, Washington, D. C., for petitioners.

Lawrence G. Wallace, Washington, D. C., for respondents.

Opinion

***386** ****681** Justice REHNQUIST delivered the opinion of the Court.

We granted certiorari in this case to address important questions concerning the scope of the attorney–client privilege in the corporate context and the applicability of the work–product doctrine in proceedings to enforce tax summonses. 445 U.S. 925, 100 S.Ct. 1310, 63 L.Ed.2d 758. With respect to the privilege question the parties and various *amici* have described our task as one of choosing between two “tests” which have gained adherents in the courts of appeals. We are acutely aware, however, that we sit to decide concrete cases and not abstract propositions of law. We decline to lay down a broad rule or series of rules to govern all conceivable future questions in this area, even were we able to do so. We can and do, however, conclude that the attorney–client privilege protects the communications involved in

this case from compelled disclosure and that the work–product doctrine does apply in tax summons enforcement proceedings.

I

Petitioner Upjohn Co. manufactures and sells pharmaceuticals here and abroad. In January 1976 independent accountants conducting an audit of one of Upjohn's foreign subsidiaries discovered that the subsidiary made payments to or for the benefit of foreign government officials in order to secure government business. The accountants, so informed petitioner, Mr. Gerard Thomas, Upjohn's Vice President, Secretary, and General Counsel. Thomas is a member of the Michigan and New York Bars, and has been Upjohn's General Counsel for 20 years. He consulted with outside counsel and R. T. Parfet, Jr., Upjohn's Chairman of the Board. It was decided that the company would conduct an internal investigation of what were termed "questionable payments." As part of this investigation the attorneys prepared a letter containing a questionnaire which was sent to "All Foreign General and Area Managers" over the Chairman's signature. The letter ***387** began by noting recent disclosures that several American companies made "possibly illegal" payments to foreign government officials and emphasized that the management needed full information concerning any such payments made by Upjohn. The letter indicated that the Chairman had asked Thomas, identified as "the company's General Counsel," "to conduct an investigation for the purpose of determining the nature and magnitude of any payments made by the Upjohn Company or any of its subsidiaries to any employee or official of a foreign government." The questionnaire sought detailed information concerning such payments. Managers were instructed to treat the investigation as "highly confidential" and not to discuss it with anyone other than Upjohn employees who might be helpful in providing the requested information. Responses were to be sent directly to Thomas. Thomas and outside counsel also interviewed the recipients of the questionnaire and some 33 other Upjohn officers or employees as part of the investigation.

On March 26, 1976, the company voluntarily submitted a preliminary report to the Securities and Exchange Commission on Form 8–K disclosing certain questionable payments.[1] A copy of the report was simultaneously submitted to the Internal Revenue Service, which immediately began an investigation to determine the tax consequences of the payments. Special agents conducting the investigation were given lists by Upjohn of all those interviewed and all who had responded to the questionnaire. On November 23, 1976, the Service issued a summons pursuant to 26 U.S.C. § 7602 demanding production of:

> "All files relative to the investigation conducted under the supervision of Gerard Thomas to identify payments to employees of foreign governments and any ****682** political ***388** contributions made by the Upjohn Company or any of its affiliates since January 1, 1971 and to determine whether any funds of the Upjohn Company had been improperly accounted for on the corporate books during the same period.
>
> > "The records should include but not be limited to written questionnaires sent to managers of the Upjohn Company's foreign affiliates, and memorandums or notes of the interviews conducted in the United States and abroad with officers and employees of the Upjohn Company and its subsidiaries." App. 17a–18a.

The company declined to produce the documents specified in the second paragraph on the grounds that they were protected from disclosure by the attorney–client privilege and constituted the work product of attorneys prepared in anticipation of litigation. On August 31, 1977, the United States filed a petition seeking enforcement of the summons under 26 U.S.C. §§ 7402(b) and 7604(a) in the United States District Court for the Western District of Michigan. That court adopted the recommendation of a Magistrate who concluded that the summons should be enforced. Petitioners appealed to the Court of Appeals for the Sixth Circuit which rejected the Magistrate's finding of a waiver of the attorney–client privilege, 600 F.2d 1223, 1227, n. 12, but agreed that the privilege did not apply "[t]o the extent that the communications were made by officers and agents not responsible for directing Upjohn's actions in response to legal advice ... for the simple reason that the communications were not the 'client's.' " *Id.*, at 1225. The court reasoned that accepting petitioners' claim for a broader application of the privilege would encourage upper–echelon management to ignore unpleasant facts and create too broad a "zone of silence." Noting that Upjohn's counsel had interviewed officials such as the Chairman and President, the Court of Appeals remanded to the District Court so that a determination of who was ***389** within the "control group" could be made. In a concluding footnote the court stated that the work–product doctrine "is not

applicable to administrative summonses issued under 26 U.S.C. § 7602." *Id.*, at 1228, n. 13.

II

[1] **[2]** Federal Rule of Evidence 501 provides that "the privilege of a witness ... shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in light of reason and experience." The attorney–client privilege is the oldest of the privileges for confidential communications known to the common law. 8 J. Wigmore, Evidence § 2290 (McNaughton rev. 1961). Its purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client. As we stated last Term in *Trammel v. United States*, 445 U.S. 40, 51, 100 S.Ct. 906, 913, 63 L.Ed.2d 186 (1980): "The lawyer–client privilege rests on the need for the advocate and counselor to know all that relates to the client's reasons for seeking representation if the professional mission is to be carried out." And in *Fisher v. United States*, 425 U.S. 391, 403, 96 S.Ct. 1569, 1577, 48 L.Ed.2d 39 (1976), we recognized the purpose of the privilege to be "to encourage clients to make full disclosure to their attorneys." This rationale for the privilege has long been recognized by the Court, see *Hunt v. Blackburn*, 128 U.S. 464, 470, 9 S.Ct. 125, 127, 32 L.Ed. 488 (1888) (privilege "is founded upon the necessity, in the interest and administration of justice, of the aid of persons having knowledge of the law and skilled in its practice, which assistance can only be safely and readily availed of when free from the consequences or the apprehension of disclosure"). Admittedly complications in the application of the privilege arise when the client is a corporation, which in theory is an artificial creature of the ***390** ****683** law, and not an individual; but this Court has assumed that the privilege applies when the client is a corporation. *United States v. Louisville & Nashville R. Co.*, 236 U.S. 318, 336, 35 S.Ct. 363, 369, 59 L.Ed. 598 (1915), and the Government does not contest the general proposition.

[3] The Court of Appeals, however, considered the application of the privilege in the corporate context to present a "different problem," since the client was an inanimate entity and "only the senior management, guiding and integrating the several operations, ... can be said to possess an identity analogous to the corporation as a whole." 600 F.2d at 1226. The first case to articulate the so–called "control group test" adopted by the court below, *Philadelphia v. Westinghouse Electric Corp.*, 210 F.Supp. 483, 485 (ED Pa.), petition for mandamus and prohibition denied *sub nom. General Electric Co. v. Kirkpatrick*, 312 F.2d 742 (CA3 1962), cert. denied, 372 U.S. 943, 83 S.Ct. 937, 9 L.Ed.2d 969 (1963), reflected a similar conceptual approach:

> "Keeping in mind that the question is, Is it the corporation which is seeking the lawyer's advice when the asserted privileged communication is made?, the most satisfactory solution, I think, is that if the employee making the communication, of whatever rank he may be, is in a position to control or even to take a substantial part in a decision about any action which the corporation may take upon the advice of the attorney, ... then, in effect, *he is (or personifies) the corporation* when he makes his disclosure to the lawyer and the privilege would apply." (Emphasis supplied.)

Such a view, we think, overlooks the fact that the privilege exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice. See *Trammel*, *supra*, at 51, 100 S.Ct., at 913; *Fisher*, *supra*, at 403, 96 S.Ct., at 1577. The first step in the resolution of any legal problem is ascertaining the factual background and sifting through the facts ***391** with an eye to the legally relevant. See ABA Code of Professional Responsibility, Ethical Consideration 4–1:

> "A lawyer should be fully informed of all the facts of the matter he is handling in order for his client to obtain the full advantage of our legal system. It is for the lawyer in the exercise of his independent professional judgment to separate the relevant and important from the irrelevant and unimportant. The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of his client not only facilitates the full development of facts essential to proper representation of the client but also encourages laymen to seek early legal assistance."

See also *Hickman v. Taylor*, 329 U.S. 495, 511, 67 S.Ct. 385, 393–394, 91 L.Ed. 451 (1947).

In the case of the individual client the provider of information and the person who acts on the lawyer's advice are one and the same. In the corporate context, however, it will frequently be employees beyond the control group as defined by the court below–"officers and agents ... responsible for directing [the company's] actions in response to legal advice"–who will possess the information needed by the corporation's lawyers. Middle–level—and indeed lower–level—employees can, by actions within the scope of their employment, embroil the corporation in serious legal difficulties, and it is only natural that these employees would have the relevant information needed by corporate counsel if he is adequately to advise the client with respect to such actual or potential difficulties. This fact was noted in *Diversified Industries, Inc. v. Meredith*, 572 F.2d 596 (CA8 1978) (en banc):

> "In a corporation, it may be necessary to glean information relevant to a legal problem from middle management or non–management personnel as well as from top executives. The attorney dealing with a complex legal problem 'is thus faced with a "Hobson's choice". If he ****684** interviews employees not having "the very highest authority", ***392** their communications to him will not be privileged. If, on the other hand, he interviews *only* those employees with the "very highest authority", he may find it extremely difficult, if not impossible, to determine what happened.' " *Id.*, at 608–609 (quoting Weinschel Corporate Employee Interviews and the Attorney–Client Privilege, 12 B.C.Ind. & Com. L.Rev. 873, 876 (1971)).

[4] The control group test adopted by the court below thus frustrates the very purpose of the privilege by discouraging the communication of relevant information by employees of the client to attorneys seeking to render legal advice to the client corporation. The attorney's advice will also frequently be more significant to noncontrol group members than to those who officially sanction the advice, and the control group test makes it more difficult to convey full and frank legal advice to the employees who will put into effect the client corporation's policy. See, *e. g.*, *Duplan Corp. v. Deering Milliken, Inc.*, 397 F.Supp. 1146, 1164 (DSC 1974) ("After the lawyer forms his or her opinion, it is of no immediate benefit to the Chairman of the Board or the President. It must be given to the corporate personnel who will apply it").

The narrow scope given the attorney–client privilege by the court below not only makes it difficult for corporate attorneys to formulate sound advice when their client is faced with a specific legal problem but also threatens to limit the valuable efforts of corporate counsel to ensure their client's compliance with the law. In light of the vast and complicated array of regulatory legislation confronting the modern corporation, corporations, unlike most individuals, "constantly go to lawyers to find out how to obey the law," Burnham, The Attorney–Client Privilege in the Corporate Arena, 24 Bus.Law. 901, 913 (1969), particularly since compliance with the law in this area is hardly an instinctive matter, see, *e. g.*, *United States v. United States Gypsum Co.*, 438 U.S. 422, 440–441, 98 S.Ct. 2864, 2875–2876, 57 L.Ed.2d 854 (1978) ("the behavior proscribed by the [Sherman] Act is ***393** often difficult to distinguish from the gray zone of socially acceptable and economically justifiable business conduct").[2] The test adopted by the court below is difficult to apply in practice, though no abstractly formulated and unvarying "test" will necessarily enable courts to decide questions such as this with mathematical precision. But if the purpose of the attorney–client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all. The very terms of the test adopted by the court below suggest the unpredictability of its application. The test restricts the availability of the privilege to those officers who play a "substantial role" in deciding and directing a corporation's legal response. Disparate decisions in cases applying this test illustrate its unpredictability. Compare, *e. g.*, *Hogan v. Zletz*, 43 F.R.D. 308, 315–316 (ND Okl.1967), aff'd in part *sub nom. Natta v. Hogan*, 392 F.2d 686 (CA10 1968) (control group includes managers and assistant managers of patent division and research and development department), with *Congoleum Industries, Inc. v. GAF Corp.*, 49 F.R.D. 82, 83–85 (ED Pa.1969), aff'd, 478 F.2d 1398 (CA3 1973) (control group includes only division and corporate ****685** vice presidents, and not two directors of research and vice president for production and research).

***394** **[5]** The communications at issue were made by Upjohn employees[3] to counsel for Upjohn acting as such, at the direction of corporate superiors in order to secure legal advice from counsel. As the Magistrate found, "Mr. Thomas consulted with the Chairman of the Board and outside counsel and thereafter conducted a factual investigation to determine the nature and extent of the questionable payments *and to be*

in a position to give legal advice to the company with respect to the payments." (Emphasis supplied.) 78–1 USTC ¶ 9277, pp. 83,598, 83,599. Information, not available from upper–echelon management, was needed to supply a basis for legal advice concerning compliance with securities and tax laws, foreign laws, currency regulations, duties to shareholders, and potential litigation in each of these areas.[4] The communications concerned matters within the scope of the employees' corporate duties, and the employees themselves were sufficiently aware that they were being questioned in order that the corporation could obtain legal advice. The questionnaire identified Thomas as "the company's General Counsel" and referred in its opening sentence to the possible illegality of payments such as the ones on which information was sought. App. 40a. A statement of policy accompanying the questionnaire clearly indicated the legal implications of the investigation. The policy statement was issued "in order that there be no uncertainty in the future as to the policy with respect to the practices which are the subject of this investigation." ***395** It began "Upjohn will comply with all laws and regulations," and stated that commissions or payments "will not be used as a subterfuge for bribes or illegal payments" and that all payments must be "proper and legal." Any future agreements with foreign distributors or agents were to be approved "by a company attorney" and any questions concerning the policy were to be referred "to the company's General Counsel." *Id.*, at 165a–166a. This statement was issued to Upjohn employees worldwide, so that even those interviewees not receiving a questionnaire were aware of the legal implications of the interviews. Pursuant to explicit instructions from the Chairman of the Board, the communications were considered "highly confidential" when made, *id.*, at 39a, 43a, and have been kept confidential by the company.[5] Consistent with the underlying purposes of the attorney–client privilege, these communications must be protected against compelled disclosure.

[6] The Court of Appeals declined to extend the attorney–client privilege beyond the limits of the control group test for fear that doing so would entail severe burdens on discovery and create a broad "zone of silence" over corporate affairs. Application of the attorney–client privilege to communications such as those involved here, however, puts the adversary in no worse position than if the communications had never taken place. The privilege only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney:

> "[T]he protection of the privilege extends only to *communications* and not to facts. A fact is one thing and a communication concerning that fact is an entirely different ****686** ***396** thing. The client cannot be compelled to answer the question, 'What did you say or write to the attorney?' but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney." *Philadelphia v. Westinghouse Electric Corp.*, 205 F.Supp. 830, 831 (q2.7).

See also *Diversified Industries*, 572 F.2d., at 611; *State ex rel. Dudek v. Circuit Court*, 34 Wis.2d 559, 580, 150 N.W.2d 387, 399 (1967) ("the courts have noted that a party cannot conceal a fact merely by revealing it to his lawyer"). Here the Government was free to question the employees who communicated with Thomas and outside counsel. Upjohn has provided the IRS with a list of such employees, and the IRS has already interviewed some 25 of them. While it would probably be more convenient for the Government to secure the results of petitioner's internal investigation by simply subpoenaing the questionnaires and notes taken by petitioner's attorneys, such considerations of convenience do not overcome the policies served by the attorney–client privilege. As Justice Jackson noted in his concurring opinion in *Hickman v. Taylor*, 329 U.S., at 516, 67 S.Ct., at 396: "Discovery was hardly intended to enable a learned profession to perform its functions ... on wits borrowed from the adversary."

[7] Needless to say, we decide only the case before us, and do not undertake to draft a set of rules which should govern challenges to investigatory subpoenas. Any such approach would violate the spirit of Federal Rule of Evidence 501. See S.Rep. No. 93–1277, p. 13 (1974) ("the recognition of a privilege based on a confidential relationship ... should be determined on a case–by–case basis"); *Trammel*, 445 U.S., at 47, 100 S.Ct., at 910–911; *United States v. Gillock*, 445 U.S. 360, 367, 100 S.Ct. 1185, 1190, 63 L.Ed.2d 454 (1980). While such a "case–by–case" basis may to some slight extent undermine desirable certainty in the boundaries of the attorney–clientt ***397** privilege, it obeys the spirit of the Rules. At the same time we conclude that the narrow "control group test" sanctioned by the Court of Appeals, in this case cannot, consistent with "the principles of the common law as ... interpreted ... in the light of reason and experience," Fed. Rule Evid. 501, govern the development of the law in this area.

III

Our decision that the communications by Upjohn employees to counsel are covered by the attorney–client privilege disposes of the case so far as the responses to the questionnaires and any notes reflecting responses to interview questions are concerned. The summons reaches further, however, and Thomas has testified that his notes and memoranda of interviews go beyond recording responses to his questions. App. 27a–28a, 91a–93a. To the extent that the material subject to the summons is not protected by the attorney–client privilege as disclosing communications between an employee and counsel, we must reach the ruling by the Court of Appeals that the work–product doctrine does not apply to summonses issued under 26 U.S.C. § 7602. [6]

[8] **[9]** **[10]** The Government concedes, wisely, that the Court of Appeals erred and that the work–product doctrine does apply to IRS summonses. Brief for Respondents 16, 48. This doctrine was announced by the Court over 30 years ago in *Hickman v. Taylor*, 329 U.S. 495, 67 S.Ct. 385, 91 L.Ed. 451 (1947). In that case the Court rejected "an attempt, without purported necessity or justification, to secure written statements, private memoranda and personal recollections prepared or formed by an adverse party's counsel in the course of his legal duties." *Id.*, at 510, 67 S.Ct., at 393. The Court noted that "it is essential that a lawyer work with ***398** a certain degree of privacy" ****687** and reasoned that if discovery of the material sought were permitted

> "much of what is now put down in writing would remain unwritten. An attorney's thoughts, heretofore inviolate, would not be his own. Inefficiency, unfairness and sharp practices would inevitably develop in the giving of legal advice and in the preparation of cases for trial. The effect on the legal profession would be demoralizing. And the interests of the clients and the cause of justice would be poorly served." *Id.*, at 511, 67 S.Ct., at 393–394.

The "strong public policy" underlying the work–product doctrine was reaffirmed recently in *United States v. Nobles*, 422 U.S. 225, 236–240, 95 S.Ct. 2160, 2169–2171, 45 L.Ed.2d 141 (1975), and has been substantially incorporated in Federal Rule of Civil Procedure 26(b)(3). [7]

As we stated last Term, the obligation imposed by a tax summons remains "subject to the traditional privileges and limitations." *United States v. Euge*, 444 U.S. 707, 714, 100 S.Ct. 874, 879–880, 63 L.Ed.2d 741 (1980). Nothing in the language of the IRS summons provisions or their legislative history suggests an intent on the part of Congress to preclude application of the work–product doctrine. Rule 26(b)(3) codifies the work–product doctrine, and the Federal Rules of Civil Procedure are made applicable ***399** to summons enforcement proceedings by Rule 81(a)(3). See *Donaldson v. United States*, 400 U.S. 517, 528, 91 S.Ct. 534, 541, 27 L.Ed.2d 580 (1971). While conceding the applicability of the work–product doctrine, the Government asserts that it has made a sufficient showing of necessity to overcome its protections. The Magistrate apparently so found, 78–1 USTC ¶ 9277, p. 83,605. The Government relies on the following language in *Hickman*:

> "We do not mean to say that all written materials obtained or prepared by an adversary's counsel with an eye toward litigation are necessarily free from discovery in all cases. Where relevant and nonprivileged facts remain hidden in an attorney's file and where production of those facts is essential to the preparation of one's case, discovery may properly be had.... And production might be justified where the witnesses are no longer available or can be reached only with difficulty." 329 U.S., at 511, 67 S.Ct., at 394.

The Government stresses that interviewees are scattered across the globe and that Upjohn has forbidden its employees to answer questions it considers irrelevant. The above–quoted language from *Hickman*, however, did not apply to "oral statements made by witnesses ... whether presently in the form of [the attorney's] mental impressions or memoranda." *Id.*, at 512, 67 S.Ct., at 394. As to such material the Court did "not believe that any showing of necessity can be made under the circumstances of this case so as to justify production.... If there should be a rare situation justifying production of these matters petitioner's case is not of that type." *Id.*, at 512–513, 67 S.Ct., at 394–395. See also *Nobles*, *supra*, 422 U.S., at 252–253, 95 S.Ct., at 2177 (WHITE, J., concurring). Forcing an attorney to disclose notes and memoranda of witnesses' oral statements is particularly disfavored because it tends to reveal the attorney's mental processes, 329 U. S., at 513, 67 S.Ct., at 394–395 ("what he saw fit to write down regarding witnesses' remarks"); *id*, at 516–517, 67 S.Ct., at 396 ****688** ("the statement would be his [the ***400** attorney's] language, permeated with his inferences") (Jackson, J., concurring). [8]

Rule 26 accords special protection to work product revealing the attorney's mental processes. The Rule permits disclosure of documents and tangible things constituting attorney work product upon a showing of substantial need and inability

to obtain the equivalent without undue hardship. This was the standard applied by the Magistrate, 78–1 USTC ¶ 9277, p. 83,604. Rule 26 goes on, however, to state that "[i]n ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions or legal theories of an attorney or other representative of a party concerning the litigation." Although this language does not specifically refer to memoranda based on oral statements of witnesses, the *Hickman* court stressed the danger that compelled disclosure of such memoranda would reveal the attorney's mental processes. It is clear that this is the sort of material the draftsmen of the Rule had in mind as deserving special protection. See Notes of Advisory Committee on 1970 Amendment to Rules, 28 U.S.C.App., p. 442 ("The subdivision ... goes on to protect against disclosure the mental impressions, conclusions, opinions, or legal theories ... of an attorney or other representative of a party. The *Hickman* opinion drew special attention to the need for protecting an attorney against discovery of memoranda prepared from recollection of oral interviews. The courts have steadfastly safeguarded against disclosure of lawyers' mental impressions and legal theories ...").

***401** Based on the foregoing, some courts have concluded that *no* showing of necessity can overcome protection of work product which is based on oral statements from witnesses. See, *e. g.*, *In re Grand Jury Proceedings*, 473 F.2d 840, 848 (CA8 1973) (personal recollections, notes, and memoranda pertaining to conversation with witnesses); *In re Grand Jury Investigation*, 412 F.Supp. 943, 949 (ED Pa.1976) (notes of conversation with witness "are so much a product of the lawyer's thinking and so little probative of the witness's actual words that they are absolutely protected from disclosure"). Those courts declining to adopt an absolute rule have nonetheless recognized that such material is entitled to special protection. See, *e. g.*, *In re Grand Jury Investigation*, 599 F.2d 1224, 1231 (CA3 1979) ("special considerations ... must shape any ruling on the discoverability of interview memoranda ...; such documents will be discoverable only in a 'rare situation' "); Cf. *In re Grand Jury Subpoena*, 599 F.2d 504, 511–512 (CA2 1979).

We do not decide the issue at this time. It is clear that the Magistrate applied the wrong standard when he concluded that the Government had made a sufficient showing of necessity to overcome the protections of the work–product doctrine. The Magistrate applied the "substantial need" and "without undue hardship" standard articulated in the first part of Rule 26(b)(3). The notes and memoranda sought by the Government here, however, are work product based on oral statements. If they reveal communications, they are, in this case, protected by the attorney–client privilege. To the extent they do not reveal communications, they reveal the attorneys' mental processes in evaluating the communications. As Rule 26 and *Hickman* make clear, such work product cannot be disclosed simply on a showing of substantial need and inability to obtain the equivalent without undue hardship.

While we are not prepared at this juncture to say that such material is always protected by the work–product rule, we ***402** ****689** think a far stronger showing of necessity and unavailability by other means than was made by the Government or applied by the Magistrate in this case would be necessary to compel disclosure. Since the Court of Appeals thought that the work–product protection was never applicable in an enforcement proceeding such as this, and since the Magistrate whose recommendations the District Court adopted applied too lenient a standard of protection, we think the best procedure with respect to this aspect of the case would be to reverse the judgment of the Court of Appeals for the Sixth Circuit and remand the case to it for such further proceedings in connection with the work–product claim as are consistent with this opinion.

Accordingly, the judgment of the Court of Appeals is reversed, and the case remanded for further proceedings.

It is so ordered.

Chief Justice BURGER, concurring in part and concurring in the judgment.

I join in Parts I and III of the opinion of the Court and in the judgment. As to Part II, I agree fully with the Court's rejection of the so–called "control group" test, its reasons for doing so, and its ultimate holding that the communications at issue are privileged. As the Court states, however, "if the purpose of the attorney–client privilege is to be served, the attorney and client must be able to predict with some degree of certainty whether particular discussions will be protected." *Ante*, at 684. For this very reason, I believe that we should articulate a standard that will govern similar cases and afford guidance to corporations, counsel advising them, and federal courts.

The Court properly relies on a variety of factors in concluding that the communications now before us are privileged. See *ante*, at 685. Because of the great importance of the issue, in

my view the Court should make clear now that, as a ***403** general rule, a communication is privileged at least when, as here, an employee or former employee speaks at the direction of the management with an attorney regarding conduct or proposed conduct within the scope of employment. The attorney must be one authorized by the management to inquire into the subject and must be seeking information to assist counsel in performing any of the following functions: (a) evaluating whether the employee's conduct has bound or would bind the corporation; (b) assessing the legal consequences, if any, of that conduct; or (c) formulating appropriate legal responses to actions that have been or may be taken by others with regard to that conduct. See, *e. g., Diversified Industries, Inc. v. Meredith*, 572 F.2d 596, 609 (CA8 1978) (en banc); *Harper & Row Publishers, Inc. v. Decker*, 423 F.2d 487, 491–492 (CA7 1970), aff'd by an equally divided Court, 400 U.S. 348, 91 S.Ct. 479, 27 L.Ed.2d 433 (1971); *Duplan Corp v. Deering Milliken, Inc.*, 397 F.Supp. 1146, 1163–1165 (DSC 1974). Other communications between employees and corporate counsel may indeed be privileged—as the petitioners and several *amici* have suggested in their proposed formulations [*] —but the need for certainty does not compel us now to prescribe all the details of the privilege in this case.

Nevertheless, to say we should not reach all facets of the privilege does not mean that we should neglect our duty to provide guidance in a case that squarely presents the question in a traditional adversary context. Indeed, because Federal Rule of Evidence 501 provides that the law of privileges "shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience," this Court has a special duty to clarify aspects of the law of privileges properly ***404** before us. Simply asserting that this failure "may to some slight extent undermine desirable certainty," *ante*, at 686, neither minimizes the consequences ****690** of continuing uncertainty and confusion nor harmonizes the inherent dissonance of acknowledging that uncertainty while declining to clarify it within the frame of issues presented.

All Citations

449 U.S. 383, 101 S.Ct. 677, 66 L.Ed.2d 584, 47 A.F.T.R.2d 81-523, 30 Fed.R.Serv.2d 1101, 81-1 USTC P 9138, Fed. Sec. L. Rep. P 97,817, 1980-81 Trade Cases P 63,797, 1981-1 C.B. 591, 7 Fed. R. Evid. Serv. 785

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Lumber Co.*, 200 U.S. 321, 337, 26 S.Ct. 282, 288, 50 L.Ed. 499.

1 On July 28, 1976, the company filed an amendment to this report disclosing further payments.

2 The Government argues that the risk of civil or criminal liability suffices to ensure that corporations will seek legal advice in the absence of the protection of the privilege. This response ignores the fact that the depth and quality of any investigations, to ensure compliance with the law would suffer, even were they undertaken. The response also proves too much, since it applies to all communications covered by the privilege: an individual trying to comply with the law or faced with a legal problem also has strong incentive to disclose information to his lawyer, yet the common law has recognized the value of the privilege in further facilitating communications.

3 Seven of the eighty-six employees interviewed by counsel had terminated their employment with Upjohn at the time of the interview. App. 33a–38a. Petitioners argue that the privilege should nonetheless apply to communications by these former employees concerning activities during their period of employment. Neither the District Court nor the Court of Appeals had occasion to address this issue, and we decline to decide it without the benefit of treatment below.

4 See *id.*, at 26a–27a, 103a, 123a–124a. See also *In re Grand Jury Investigation*, 599 F.2d 1224, 1229 (CA3 1979); *In re Grand Jury Subpoena*, 599 F.2d 504, 511 (CA2 1979).

5 See Magistrate's opinion, 78–1 USTC ¶ 9277, p. 83,599: "The responses to the questionnaires and the notes of the interviews have been treated as confidential material and have not been disclosed to anyone except Mr. Thomas and outside counsel."

6 The following discussion will also be relevant to counsel's notes and memoranda of interviews with the seven former employees should it be determined that the attorney–client privilege does not apply to them. See n. 3, *supra.*

7 This provides, in pertinent part:

> "[A] party may obtain discovery of documents and tangible things otherwise discoverable under subdivision (b)(1) of this rule and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including his attorney, consultant,

> surety, indemnitor, insurer, or agent) only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation."

8 Thomas described his notes of the interviews as containing "what I considered to be the important questions, the substance of the responses to them, my beliefs as to the importance of these, my beliefs as to how they related to the inquiry, my thoughts as to how they related to other questions. In some instances they might even suggest other questions that I would have to ask or things that I needed to find elsewhere." 78–1 USTC ¶ 9277, p. 83,599.

* See Brief for Petitioners 21–23, and n. 25; Brief for American Bar Association as *Amicus Curiae* 5–6, and n. 2; Brief for American College of Trial Lawyers and 33 Law Firms as *Amici Curiae* 9–10, and n. 5.

EXHIBIT E

756 F.3d 754
United States Court of Appeals,
District of Columbia Circuit.

In re KELLOGG BROWN & ROOT, INC., et al., Petitioners.

No. 14–5055.
|
Argued May 7, 2014.
|
Decided June 27, 2014.
|
Rehearing En Banc Denied Sept. 2, 2014.

Synopsis

Background: In a relator's qui tam action against a defense contractor under the False Claims Act (FCA), the United States District Court for the District of Columbia, James S. Gwin, J., 2014 WL 1016784, ordered the contractor to turn over the results of an internal investigation, and denied a stay pending appeal, 2014 WL 929430. The contractor petitioned for writ of mandamus.

Holdings: The Court of Appeals, Kavanaugh, Circuit Judge, held that:

[1] the internal investigation was protected by attorney-client privilege;

[2] the contractor had no adequate means to attain relief outside seeking a writ of mandamus;

[3] the District Court's error in denying attorney-client privilege was clear;

[4] the totality of the circumstances supported grant of a writ of mandamus; and

[5] the case did not warrant reassignment on remand.

Petition granted.

***755** On Petition for Writ of Mandamus (No. 1:05–cv–1276).

Attorneys and Law Firms

John P. Elwood argued the cause for petitioners. With him on the petition for writ of mandamus and the reply were John M. Faust, Craig D. Margolis, Jeremy C. Marwell, and Joshua S. Johnson.

Rachel L. Brand, Steven P. Lehotsky, Quentin Riegel, Carl Nichols, Elisebeth C. Cook, Adam I. Klein, Amar Sarwal, and Wendy E. Ackerman were on the brief for amicus curiae Chamber of Commerce of the United States of America, et al. in support of petitioners.

Stephen M. Kohn argued the cause for respondent. With him on the response to the petition for writ of mandamus were David K. Colapinto and Michael Kohn.

Before: GRIFFITH, KAVANAUGH, and SRINIVASAN, Circuit Judges.

Opinion

Opinion for the Court filed by Circuit Judge KAVANAUGH.

***756** KAVANAUGH, Circuit Judge:

****384** More than three decades ago, the Supreme Court held that the attorney-client privilege protects confidential employee communications made during a business's internal investigation led by company lawyers. *See Upjohn Co. v. United States,* 449 U.S. 383, 101 S.Ct. 677, 66 L.Ed.2d 584 (1981). In this case, the District Court denied the protection of the privilege to a company that had conducted just such an internal investigation. The District Court's decision has generated substantial uncertainty about the scope of the attorney-client privilege in the business setting. We conclude that the District Court's decision is irreconcilable with *Upjohn.* We therefore grant KBR's petition for a writ of mandamus and vacate the District Court's March 6 document production order.

I

Harry Barko worked for KBR, a defense contractor. In 2005, he filed a False Claims Act complaint against KBR and KBR-related corporate entities, whom we will collectively refer to as KBR. In essence, Barko alleged that KBR and certain subcontractors defrauded the U.S. Government by inflating costs and accepting kickbacks while administering military

contracts in wartime Iraq. During discovery, Barko sought documents related to KBR's prior internal investigation into the alleged fraud. KBR had conducted that internal investigation pursuant to its Code of Business Conduct, which is overseen by the company's Law Department.

KBR argued that the internal investigation had been conducted for the purpose of obtaining legal advice and that the internal investigation documents therefore were protected by the attorney-client privilege. Barko responded that the internal investigation documents were unprivileged business records that he was entitled to discover. *See generally* Fed.R.Civ.P. 26(b)(1).

After reviewing the disputed documents *in camera*, the District Court determined that the attorney-client privilege protection did not apply because, among other reasons, KBR had not shown that "the communication would not have been made 'but for' the fact that legal advice was sought." *United States ex rel. Barko v. Halliburton Co.*, No. 1:05–cv–1276, —— F.3d ——, ——, 2014 WL 1016784, at *2 (D.D.C. Mar. 6, 2014) (quoting *United States v. ISS Marine Services, Inc.*, 905 F.Supp.2d 121, 128 (D.D.C.2012)). KBR's internal investigation, the court concluded, was "undertaken pursuant to regulatory law and corporate policy rather than for the purpose of obtaining legal advice." *Id.* at ——, 2014 WL 1016784, at *3.

KBR vehemently opposed the ruling. The company asked the District Court to certify the privilege question to this Court for interlocutory appeal and to stay its order pending a petition for mandamus in this Court. The District Court denied those requests and ordered KBR to produce the disputed documents to Barko within a matter of days. *See United States ex rel. Barko v. Halliburton Co.*, No. 1:05–cv–1276, 2014 WL 929430 (D.D.C. Mar. 11, 2014). KBR promptly filed a petition for a writ of mandamus in this Court. A number of business organizations and trade associations also objected to the District Court's decision and filed an amicus brief in support of KBR. We stayed the District Court's document production order and held oral argument on the mandamus petition.

The threshold question is whether the District Court's privilege ruling constituted legal error. If not, mandamus is of course inappropriate. If the District Court's ruling was erroneous, the remaining ****385 *757** question is whether that error is the kind that justifies mandamus. *See Cheney v. U.S. District Court for the District of Columbia*, 542 U.S. 367, 380–81, 124 S.Ct. 2576, 159 L.Ed.2d 459 (2004). We address those questions in turn.

II

[1] We first consider whether the District Court's privilege ruling was legally erroneous. We conclude that it was.

Federal Rule of Evidence 501 provides that claims of privilege in federal courts are governed by the "common law—as interpreted by United States courts in the light of reason and experience." Fed.R.Evid. 501. The attorney-client privilege is the "oldest of the privileges for confidential communications known to the common law." *Upjohn Co. v. United States*, 449 U.S. 383, 389, 101 S.Ct. 677, 66 L.Ed.2d 584 (1981). As relevant here, the privilege applies to a confidential communication between attorney and client if that communication was made for the purpose of obtaining or providing legal advice to the client. *See* 1 RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §§ 68–72 (2000); *In re Grand Jury*, 475 F.3d 1299, 1304 (D.C.Cir.2007); *In re Lindsey*, 158 F.3d 1263, 1270 (D.C.Cir.1998); *In re Sealed Case*, 737 F.2d 94, 98–99 (D.C.Cir.1984); *see also Fisher v. United States*, 425 U.S. 391, 403, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976) ("Confidential disclosures by a client to an attorney made in order to obtain legal assistance are privileged.").

In *Upjohn*, the Supreme Court held that the attorney-client privilege applies to corporations. The Court explained that the attorney-client privilege for business organizations was essential in light of "the vast and complicated array of regulatory legislation confronting the modern corporation," which required corporations to "constantly go to lawyers to find out how to obey the law, ... particularly since compliance with the law in this area is hardly an instinctive matter." 449 U.S. at 392, 101 S.Ct. 677 (internal quotation marks and citation omitted). The Court stated, moreover, that the attorney-client privilege "exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice." *Id.* at 390, 101 S.Ct. 677. That is so, the Court said, because the "first step in the resolution of any legal problem is ascertaining the factual background and sifting through the facts with an eye to the legally relevant." *Id.* at 390–91, 101 S.Ct. 677. In *Upjohn*, the communications were made by company employees to company attorneys during an attorney-led

internal investigation that was undertaken to ensure the company's "compliance with the law." *Id.* at 392, 101 S.Ct. 677; *see id.* at 394, 101 S.Ct. 677. The Court ruled that the privilege applied to the internal investigation and covered the communications between company employees and company attorneys.

KBR's assertion of the privilege in this case is materially indistinguishable from Upjohn's assertion of the privilege in that case. As in *Upjohn,* KBR initiated an internal investigation to gather facts and ensure compliance with the law after being informed of potential misconduct. And as in *Upjohn,* KBR's investigation was conducted under the auspices of KBR's in-house legal department, acting in its legal capacity. The same considerations that led the Court in *Upjohn* to uphold the corporation's privilege claims apply here.

The District Court in this case initially distinguished *Upjohn* on a variety of grounds. But none of those purported distinctions takes this case out from under *Upjohn* 's umbrella.

***758 [2] **386** First, the District Court stated that in Upjohn the internal investigation began after in-house counsel conferred with outside counsel, whereas here the investigation was conducted in-house without consultation with outside lawyers. But Upjohn does not hold or imply that the involvement of outside counsel is a necessary predicate for the privilege to apply. On the contrary, the general rule, which this Court has adopted, is that a lawyer's status as in-house counsel "does not dilute the privilege." *In re Sealed Case,* 737 F.2d at 99. As the Restatement's commentary points out, "Inside legal counsel to a corporation or similar organization ... is fully empowered to engage in privileged communications." 1 RESTATEMENT § 72, cmt. c, at 551.

[3] Second, the District Court noted that in Upjohn the interviews were conducted by attorneys, whereas here many of the interviews in KBR's investigation were conducted by non-attorneys. But the investigation here was conducted at the direction of the attorneys in KBR's Law Department. And communications made by and to non-attorneys serving as agents of attorneys in internal investigations are routinely protected by the attorney-client privilege. *See FTC v. TRW, Inc.,* 628 F.2d 207, 212 (D.C.Cir.1980); *see also* 1 PAUL R. RICE, ATTORNEY–CLIENT PRIVILEGE IN THE UNITED STATES § 7:18, at 1230–31 (2013) ("If internal investigations are conducted by agents of the client at the behest of the attorney, they are protected by the attorney-client privilege to the same extent as they would be had they been conducted by the attorney who was consulted."). So that fact, too, is not a basis on which to distinguish *Upjohn.*

Third, the District Court pointed out that in *Upjohn* the interviewed employees were expressly informed that the purpose of the interview was to assist the company in obtaining legal advice, whereas here they were not. The District Court further stated that the confidentiality agreements signed by KBR employees did not mention that the purpose of KBR's investigation was to obtain legal advice. Yet nothing in *Upjohn* requires a company to use magic words to its employees in order to gain the benefit of the privilege for an internal investigation. And in any event, here as in *Upjohn* employees knew that the company's legal department was conducting an investigation of a sensitive nature and that the information they disclosed would be protected. *Cf. Upjohn,* 449 U.S. at 387, 101 S.Ct. 677 (Upjohn's managers were "instructed to treat the investigation as 'highly confidential' "). KBR employees were also told not to discuss their interviews "without the specific advance authorization of KBR General Counsel." *United States ex rel. Barko v. Halliburton Co.,* No. 1:05–cv–1276 —— F.3d ——, —— n. 33, 2014 WL 1016784, at *3 n. 33 (D.D.C. Mar. 6, 2014).

In short, none of those three distinctions of *Upjohn* holds water as a basis for denying KBR's privilege claim.

More broadly and more importantly, the District Court also distinguished *Upjohn* on the ground that KBR's internal investigation was undertaken to comply with Department of Defense regulations that require defense contractors such as KBR to maintain compliance programs and conduct internal investigations into allegations of potential wrongdoing. The District Court therefore concluded that the purpose of KBR's internal investigation was to comply with those regulatory requirements rather than to obtain or provide legal advice. In our view, the District Court's analysis rested on a false dichotomy. So long as obtaining or providing legal advice was one of the significant purposes of the internal investigation, the attorney ****387 *759** privilege applies, even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of company discretion.

The District Court began its analysis by reciting the "primary purpose" test, which many courts (including this one) have used to resolve privilege disputes when attorney-client

communications may have had both legal and business purposes. *See id.* at *2; *see also In re Sealed Case*, 737 F.2d at 98–99. But in a key move, the District Court then said that the primary purpose of a communication is to obtain or provide legal advice only if the communication would not have been made "but for" the fact that legal advice was sought. 2014 WL 1016784, at *2. In other words, if there was any other purpose behind the communication, the attorney-client privilege apparently does not apply. The District Court went on to conclude that KBR's internal investigation was "undertaken pursuant to regulatory law and corporate policy rather than for the purpose of obtaining legal advice." *Id.* at *3; *see id.* at *3 n. 28 (citing federal contracting regulations). Therefore, in the District Court's view, "the primary purpose of" the internal investigation "was to comply with federal defense contractor regulations, not to secure legal advice." *United States ex rel. Barko v. Halliburton Co.*, No. 1:05–cv–1276, 4 F.Supp.3d 162, 166, 2014 WL 929430, at *2 (D.D.C. Mar. 11, 2014); *see id.* ("Nothing suggests the reports were prepared to obtain legal advice. Instead, the reports were prepared to try to comply with KBR's obligation to report improper conduct to the Department of Defense.").

The District Court erred because it employed the wrong legal test. The but-for test articulated by the District Court is not appropriate for attorney-client privilege analysis. Under the District Court's approach, the attorney-client privilege apparently would not apply unless the sole purpose of the communication was to obtain or provide legal advice. That is not the law. We are aware of no Supreme Court or court of appeals decision that has adopted a test of this kind in this context. The District Court's novel approach to the attorney-client privilege would eliminate the attorney-client privilege for numerous communications that are made for both legal and business purposes and that heretofore have been covered by the attorney-client privilege. And the District Court's novel approach would eradicate the attorney-client privilege for internal investigations conducted by businesses that are required by law to maintain compliance programs, which is now the case in a significant swath of American industry. In turn, businesses would be less likely to disclose facts to their attorneys and to seek legal advice, which would "limit the valuable efforts of corporate counsel to ensure their client's compliance with the law." *Upjohn*, 449 U.S. at 392, 101 S.Ct. 677. We reject the District Court's but-for test as inconsistent with the principle of *Upjohn* and longstanding attorney-client privilege law.

Given the evident confusion in some cases, we also think it important to underscore that the primary purpose test, sensibly and properly applied, cannot and does not draw a rigid distinction between a legal purpose on the one hand and a business purpose on the other. After all, trying to find *the* one primary purpose for a communication motivated by two sometimes overlapping purposes (one legal and one business, for example) can be an inherently impossible task. It is often not useful or even feasible to try to determine whether the purpose was A or B when the purpose was A and B. It is thus not correct for a court to presume that a communication can have only one primary purpose ****388 *760** It is likewise not correct for a court to try to find *the* one primary purpose in cases where a given communication plainly has multiple purposes. Rather, it is clearer, more precise, and more predictable to articulate the test as follows: Was obtaining or providing legal advice *a* primary purpose of the communication, meaning one of the significant purposes of the communication? As the Reporter's Note to the Restatement says, "In general, American decisions agree that the privilege applies if one of the significant purposes of a client in communicating with a lawyer is that of obtaining legal assistance." 1 RESTATEMENT § 72, Reporter's Note, at 554. We agree with and adopt that formulation—"one of the significant purposes"—as an accurate and appropriate description of the primary purpose test. Sensibly and properly applied, the test boils down to whether obtaining or providing legal advice was one of the significant purposes of the attorney-client communication.

[4] In the context of an organization's internal investigation, if one of the significant purposes of the internal investigation was to obtain or provide legal advice, the privilege will apply. That is true regardless of whether an internal investigation was conducted pursuant to a company compliance program required by statute or regulation, or was otherwise conducted pursuant to company policy. *Cf.* Andy Liu et al., *How To Protect Internal Investigation Materials from Disclosure*, 56 GOVERNMENT CONTRACTOR ¶ 108 (Apr. 9, 2014) ("Helping a corporation comply with a statute or regulation—although required by law—does not transform quintessentially legal advice into business advice.").

In this case, there can be no serious dispute that one of the significant purposes of the KBR internal investigation was to obtain or provide legal advice. In denying KBR's privilege claim on the ground that the internal investigation was conducted in order to comply with regulatory requirements and corporate policy and not just to obtain or provide legal

advice, the District Court applied the wrong legal test and clearly erred.

III

[5] Having concluded that the District Court's privilege ruling constituted error, we still must decide whether that error justifies a writ of mandamus. *See* 28 U.S.C. § 1651. Mandamus is a "drastic and extraordinary" remedy "reserved for really extraordinary causes." *Cheney v. U.S. District Court for the District of Columbia*, 542 U.S. 367, 380, 124 S.Ct. 2576, 159 L.Ed.2d 459 (2004) (quoting *Ex parte Fahey*, 332 U.S. 258, 259–60, 67 S.Ct. 1558, 91 L.Ed. 2041 (1947)). In keeping with that high standard, the Supreme Court in *Cheney* stated that three conditions must be satisfied before a court grants a writ of mandamus: (1) the mandamus petitioner must have "no other adequate means to attain the relief he desires," (2) the mandamus petitioner must show that his right to the issuance of the writ is "clear and indisputable," and (3) the court, "in the exercise of its discretion, must be satisfied that the writ is appropriate under the circumstances." *Id.* at 380–81, 124 S.Ct. 2576 (quoting and citing *Kerr v. United States District Court for the Northern District of California*, 426 U.S. 394, 403, 96 S.Ct. 2119, 48 L.Ed.2d 725 (1976)). We conclude that all three conditions are satisfied in this case.

A

[6] **[7]** First, a mandamus petitioner must have "no other adequate means to attain the relief he desires." *Cheney*, 542 U.S. at 380, 124 S.Ct. 2576. That initial requirement will often be met in cases where a petitioner claims that a district ****389** ***761** court erroneously ordered disclosure of attorney-client privileged documents. That is because (i) an interlocutory appeal is not available in attorney-client privilege cases (absent district court certification) and (ii) appeal after final judgment will come too late because the privileged communications will already have been disclosed pursuant to the district court's order.

The Supreme Court has ruled that an interlocutory appeal under the collateral order doctrine is not available in attorney-client privilege cases. *See Mohawk Industries, Inc. v. Carpenter*, 558 U.S. 100, 106–13, 130 S.Ct. 599, 175 L.Ed.2d 458 (2009); *see also* 28 U.S.C. § 1291. To be sure, a party in KBR's position may ask the district court to certify the privilege question for interlocutory appeal. *See* 28 U.S.C. § 1292(b). But that avenue is available only at the discretion of the district court. And here, the District Court denied KBR's request for certification. *See United States ex rel. Barko v. Halliburton Co.*, No. 1:05–cv–1276, 4 F.Supp.3d 162, 165–68, 2014 WL 929430, at *1–3 (D.D.C. Mar. 11, 2014). It is also true that a party in KBR's position may defy the district court's ruling and appeal if the district court imposes contempt sanctions for non-disclosure. But as this Court has explained, forcing a party to go into contempt is not an "adequate" means of relief in these circumstances. *See In re Sealed Case*, 151 F.3d 1059, 1064–65 (D.C.Cir.1998); *see also In re City of New York*, 607 F.3d 923, 934 (2d Cir.2010) (same).

On the other hand, appeal after final judgment will often come too late because the privileged materials will already have been released. In other words, "the cat is out of the bag." *In re Papandreou*, 139 F.3d 247, 251 (D.C.Cir.1998). As this Court and others have explained, post-release review of a ruling that documents are unprivileged is often inadequate to vindicate a privilege the very purpose of which is to prevent the release of those confidential documents. *See id.; see also In re Sims*, 534 F.3d 117, 129 (2d Cir.2008) ("a remedy after final judgment cannot unsay the confidential information that has been revealed") (quoting *In re von Bulow*, 828 F.2d 94, 99 (2d Cir.1987)).

For those reasons, the first condition for mandamus—no other adequate means to obtain relief—will often be satisfied in attorney-client privilege cases. Barko responds that the Supreme Court in *Mohawk*, although addressing only the availability of interlocutory appeal under the collateral order doctrine, in effect also barred the use of mandamus in attorney-client privilege cases. According to Barko, *Mohawk* means that the first prong of the mandamus test cannot be met in attorney-client privilege cases because of the availability of post-judgment appeal. That is incorrect. It is true that *Mohawk* held that attorney-client privilege rulings are not appealable under the collateral order doctrine because "postjudgment appeals generally suffice to protect the rights of litigants and ensure the vitality of the attorney-client privilege." 558 U.S. at 109, 130 S.Ct. 599. But at the same time, the Court repeatedly and expressly reaffirmed that *mandamus*—as opposed to the collateral order doctrine—remains a "useful safety valve" in some cases of clear error to correct "some of the more consequential attorney-client privilege rulings." *Id.* at 110–12, 130 S.Ct. 599 (internal quotation marks and alteration omitted). It would make little sense to read *Mohawk* to implicitly preclude mandamus review in all cases given that *Mohawk* explicitly preserved mandamus review

in some cases. Other appellate courts that have considered this question have agreed. *See Hernandez v. Tanninen*, 604 F.3d 1095, 1101 (9th Cir.2010); *In re Whirlpool Corp.*, 597 F.3d 858, 860 (7th Cir.2010); *see also In* ****390 *762** *re Perez*, 749 F.3d 849 (9th Cir.2014) (granting mandamus after *Mohawk* on informants privilege ruling); *City of New York*, 607 F.3d at 933 (same on law enforcement privilege ruling).

B

[8] [9] [10] Second, a mandamus petitioner must show that his right to the issuance of the writ is "clear and indisputable." *Cheney*, 542 U.S. at 381, 124 S.Ct. 2576. Although the first mandamus requirement is often met in attorney-client privilege cases, this second requirement is rarely met. An erroneous district court ruling on an attorney-client privilege issue by itself does not justify mandamus. The error has to be clear. As a result, appellate courts will often deny interlocutory mandamus petitions advancing claims of error by the district court on attorney-client privilege matters. In this case, for the reasons explained at length in Part II, we conclude that the District Court's privilege ruling constitutes a clear legal error. The second prong of the mandamus test is therefore satisfied in this case.

C

[11] [12] Third, before granting mandamus, we must be "satisfied that the writ is appropriate under the circumstances." *Cheney*, 542 U.S. at 381, 124 S.Ct. 2576. As its phrasing suggests, that is a relatively broad and amorphous totality of the circumstances consideration. The upshot of the third factor is this: Even in cases of clear district court error on an attorney-client privilege matter, the circumstances may not always justify mandamus.

In this case, considering all of the circumstances, we are convinced that mandamus is appropriate. The District Court's privilege ruling would have potentially far-reaching consequences. In distinguishing *Upjohn*, the District Court relied on a number of factors that threaten to vastly diminish the attorney-client privilege in the business setting. Perhaps most importantly, the District Court's distinction of *Upjohn* on the ground that the internal investigation here was conducted pursuant to a compliance program mandated by federal regulations would potentially upend certain settled understandings and practices. Because defense contractors are subject to regulatory requirements of the sort cited by the District Court, the logic of the ruling would seemingly prevent any defense contractor from invoking the attorney-client privilege to protect internal investigations undertaken as part of a mandatory compliance program. *See* 48 C.F.R. § 52.203–13 (2010). And because a variety of other federal laws require similar internal controls or compliance programs, many other companies likewise would not be able to assert the privilege to protect the records of their internal investigations. *See, e.g.*, 15 U.S.C. §§ 78m(b)(2), 7262; 41 U.S.C. § 8703. As KBR explained, the District Court's decision "would disable *most public companies* from undertaking confidential internal investigations." KBR Pet. 19. As amici added, the District Court's novel approach has the potential to "work a sea change in the well-settled rules governing internal corporate investigations." Br. of Chamber of Commerce et al. as Amici Curaie 1; *see* KBR Reply Br. 1 n. 1 (citing commentary to same effect); Andy Liu et al., *How To Protect Internal Investigation Materials from Disclosure*, 56 GOVERNMENT CONTRACTOR ¶ 108 (Apr. 9, 2014) (assessing broad impact of ruling on government contractors).

To be sure, there are limits to the impact of a single district court ruling because it is not binding on any other court or judge. But prudent counsel monitor court decisions closely and adapt their ****391 *763** practices in response. The amicus brief in this case, which was joined by numerous business and trade associations, convincingly demonstrates that many organizations are well aware of and deeply concerned about the uncertainty generated by the novelty and breadth of the District Court's reasoning. That uncertainty matters in the privilege context, for the Supreme Court has told us that an "uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all." *Upjohn Co. v. United States*, 449 U.S. 383, 393, 101 S.Ct. 677, 66 L.Ed.2d 584 (1981). More generally, this Court has long recognized that mandamus can be appropriate to " forestall future error in trial courts" and "eliminate uncertainty" in important areas of law. *Colonial Times, Inc. v. Gasch*, 509 F.2d 517, 524 (D.C.Cir.1975). Other courts have granted mandamus based on similar considerations. *See In re Sims*, 534 F.3d 117, 129 (2d Cir.2008) (granting mandamus where "immediate resolution will avoid the development of discovery practices or doctrine undermining the privilege") (quotation omitted); *In re Seagate Technology, LLC*, 497 F.3d 1360, 1367 (Fed.Cir.2007) (en banc) (same). The novelty of the District Court's privilege ruling, combined with its potentially broad and destabilizing effects in an important

area of law, convinces us that granting the writ is "appropriate under the circumstances." *Cheney*, 542 U.S. at 381, 124 S.Ct. 2576. In saying that, we do not mean to imply that all of the circumstances present in this case are necessary to meet the third prong of the mandamus test. But they are sufficient to do so here. We therefore grant KBR's petition for a writ of mandamus.

IV

[13] We have one final matter to address. At oral argument, KBR requested that if we grant mandamus, we also reassign this case to a different district court judge. *See* Tr. of Oral Arg. at 17–19; 28 U.S.C. § 2106. KBR grounds its request on the District Court's erroneous decisions on the privilege claim, as well as on a letter sent by the District Court to the Clerk of this Court in which the District Court arranged to transfer the record in the case and identified certain documents as particularly important for this Court's review. *See* KBR Reply Br.App. 142. KBR claims that the letter violated Federal Rule of Appellate Procedure 21(b)(4), which provides that in a mandamus proceeding the "trial-court judge may request permission to address the petition but may not do so unless invited or ordered to do so by the court of appeals."

[14] In its mandamus petition, KBR did not request reassignment. Nor did KBR do so in its reply brief, even though the company knew by that time of the District Court letter that it complains about. Ordinarily, we do not consider a request for relief that a party failed to clearly articulate in its briefs. To be sure, appellate courts on rare occasions will reassign a case sua sponte. *See Ligon v. City of New York*, 736 F.3d 118, 129 & n. 31 (2d Cir.2013) (collecting cases), *vacated in part*, 743 F.3d 362 (2d Cir.2014). But whether requested to do so or considering the matter sua sponte, we will reassign a case only in the exceedingly rare circumstance that a district judge's conduct is "so extreme as to display clear inability to render fair judgment." *Liteky v. United States*, 510 U.S. 540, 551, 114 S.Ct. 1147, 127 L.Ed.2d 474 (1994); *see also United States v. Microsoft Corp.*, 253 F.3d 34, 107 (D.C.Cir.2001) (en banc). Nothing in the District Court's decisions or subsequent letter reaches that very high standard. Based on the record before us, we have no reason to doubt that the District Court will ****392** ***764** render fair judgment in further proceedings. We will not reassign the case.

* * *

In reaching our decision here, we stress, as the Supreme Court did in *Upjohn*, that the attorney-client privilege "only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney." *Upjohn Co. v. United States*, 449 U.S. 383, 395, 101 S.Ct. 677, 66 L.Ed.2d 584 (1981). Barko was able to pursue the facts underlying KBR's investigation. But he was not entitled to KBR's own investigation files. As the *Upjohn* Court stated, quoting Justice Jackson, "Discovery was hardly intended to enable a learned profession to perform its functions ... on wits borrowed from the adversary." *Id.* at 396, 101 S.Ct. 677 (quoting *Hickman v. Taylor*, 329 U.S. 495, 515, 67 S.Ct. 385, 91 L.Ed. 451 (1947) (Jackson, J., concurring)).

Although the attorney-client privilege covers only communications and not facts, we acknowledge that the privilege carries costs. The privilege means that potentially critical evidence may be withheld from the factfinder. Indeed, as the District Court here noted, that may be the end result in this case. But our legal system tolerates those costs because the privilege "is intended to encourage 'full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice.' " *Swidler & Berlin v. United States*, 524 U.S. 399, 403, 118 S.Ct. 2081, 141 L.Ed.2d 379 (1998) (quoting *Upjohn*, 449 U.S. at 389, 101 S.Ct. 677).

We grant the petition for a writ of mandamus and vacate the District Court's March 6 document production order. To the extent that Barko has timely asserted other arguments for why these documents are not covered by either the attorney-client privilege or the work-product protection, the District Court may consider such arguments.

So ordered.

All Citations

756 F.3d 754, 410 U.S.App.D.C. 382, 38 IER Cases 1109, 94 Fed. R. Evid. Serv. 1078, 94 Fed. R. Evid. Serv. 1129

End of Document

EXHIBIT F

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation.

MDL No. 14-2522 (PAM/JJK)

ORDER

This document relates to Financial Institution Actions.

This matter is before the Court on the Plaintiffs' request for the Court's intervention in compelling Target to produce certain documents that Target withheld from production and identified on its privilege log. Plaintiffs assert that Target improperly raised claims of attorney-client privilege and work-product protection for the items identified on the privilege log. (Doc. No. 593, Pls.' Letter Br.; *see also id.*, Appendix A, Pls.' Privilege Log Challenges (raising challenges to 370 entries on Target's initial privilege log).) Plaintiffs assert that Target improperly asserted privilege and work-product claims for items relating to a group called the Data Breach Task Force, which Target established in response to the data breach that precipitated this multi-district litigation. Plaintiffs also contend that Target improperly asserted privilege and work-product claims for communications with and documents prepared by Verizon. Target retained Verizon to investigate the data breach. Plaintiffs argue that these communications and documents at issue are not protected by the attorney-client privilege and the work-product doctrine because "Target would have had to investigate and fix the data breach regardless of any litigation, to appease its customers and ensure continued

sales, discover its vulnerabilities, and protect itself against future breaches." (Pls.' Letter Br. 3–4.)

Target opposes the Plaintiffs' motion to compel production of these allegedly privileged and work-product protected communications and documents, and filed a letter brief (Doc. No. 599, Target's Letter Br.), along with several declarations and exhibits to substantiate Target's privilege and work-product claims (Doc. Nos. 600–04). Target asserts that the Data Breach Task Force was not involved in an ordinary-course-of-business investigation of the data breach. Rather, Target alleges that it established the Data Breach Task Force at the request of Target's in-house lawyers and its retained outside counsel so that the task force could educate Target's attorneys about aspects of the breach and counsel could provide Target with informed legal advice. (*See* Target's Letter Br. 1–2.) Target's Chief Legal Officer, Timothy Baer, Esq., explains that shortly after discovering the possibility that a data breach had occurred, Target retained outside counsel to obtain legal advice about the breach and its possible legal ramifications. (Doc. No. 600, Decl. of Timothy Baer, Esq. ("Baer Decl.") ¶¶ 4–5.) Once Target publicly announced the breach, consumers filed several class action lawsuits against Target (*id.* ¶ 8), and in early January 2014, Target established the Data Breach Task Force "to coordinate activities on behalf of [Target's in-house and outside] counsel to better position the Target Law Department and outside counsel to provide legal advice to Target personnel to defend the company" (*id.* ¶ 9).

With respect to Verizon, Target also explains that it has only claimed privilege and work-product protection for documents involving one team from Verizon Business

Network Services, which Target's outside counsel engaged to "'enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries.'" (Target's Letter Br. 4 (quoting Doc. No. 603, Decl. of Miriam Wugmeister, Esq. ("Wugmeister Decl.") ¶ 11; *see also* Doc. No. 604, Decl. of Michelle Visser, Esq. ("Visser Decl.") ¶ 3 n.1 (explaining that Ropes & Gray LLP was a party to an engagement letter entered into with a team from Verizon Business Network Services).) Meanwhile, another team from Verizon also conducted a separate investigation into the data breach on behalf of several credit card brands. (*See* Wugmeister Decl. ¶ 11; *see also* Doc. No. 602, Decl. of David Ostertag ¶ 10 (describing a separate investigation conducted by Verizon "on behalf of the payment card brands" and explaining that the Verizon teams did not communicate with each other about the substance of the attorney-directed investigation).)

In other words, Target asserts that following the data breach, there was a two-track investigation. On one track, it conducted its own ordinary-course investigation, and a team from Verizon conducted a non-privileged investigation on behalf of credit card companies. This track was set up so that Target and Verizon could learn how the breach happened and Target (and apparently the credit card brands) could respond to it appropriately. On the other track, Target's lawyers needed to be educated about the breach so that they could provide Target with legal advice and protect the company's interests in litigation that commenced almost immediately after the breach became publicly known. On this second track, Target established its own task force and engaged a separate team from Verizon to provide counsel with the necessary input, and it is for

information generated along this track that Target has claimed attorney-client privilege and work-product protection.

Given the scope of the communications and documents at issue and so the Court would not be evaluating the parties' positions in a vacuum, on October 13, 2015, the Court ordered Target to provide certain documents for in camera inspection. (Doc. No. 618.) Specifically, the Court instructed Target to provide it with the documents identified in the bulleted list on pages 4 and 5 of the Plaintiffs' Letter Brief. Target provided the documents[1] in camera, and the Court has completed its in camera review. Based on that in camera review, the Court concludes that no hearing is required to decide the privilege and work-product issues raised as to the specific examples listed in Plaintiffs' Letter Brief. The Court limits its ruling in this Order to the specific privilege log entries that Target submitted for in camera review. The Court makes no ruling about any other entry on Target's privilege log. The parties may take guidance from this Order in their attempts to resolve their remaining disputes concerning Target's other claims of privilege and work-product protection.

Accordingly, **IT IS HEREBY ORDERED** that Plaintiffs' Motion to Compel (Doc. No. 593) is **GRANTED IN PART** and **DENIED IN PART** as follows:

1. The motion is **GRANTED IN PART** to the extent it seeks production of the redacted information corresponding to Target's privilege log entries 763–64, and

[1] Although the Court's October 13th Order mentioned 36 "documents" that were identified in Plaintiffs' Letter Brief, based on the in camera review, it is clear that the privilege log entries correspond to redactions, and some of these documents include multiple redactions, which correspond to multiple entries on Target's privilege log.

988–89. Target redacted information in these email communications that are updates to Target's Board of Directors in the aftermath of the data breach. These redacted communications from Target's Chief Executive Officer merely update the Board of Directors on what Target's business-related interests were in response to the breach. Nothing in the record supports a claim for attorney-client privilege for these communications as they do not involve any confidential communications between attorney and client, contain requests for or discussion necessary to obtain legal advice, nor include the provision of legal advice. Nor does anything in the record support a claim of work-product protection for this Board of Directors update. None of Target's declarations demonstrates that this Board of Directors update was provided because of any anticipation of litigation within the meaning of Fed. R. Civ. P. 26(b)(3). Target must provide unredacted versions of the emails corresponding to privilege log entries 763–64 and 988–89 within 3 days of this Order.

2. Otherwise, based on the Court's in camera review, and the declarations in support of Target's opposition, Plaintiffs' motion is **DENIED** with respect to the other privilege log entries that were included in Target's in camera submission:

a. The motion is moot with respect to entries 1360–65 on Target's privilege log. Target represented that the emails corresponding to those entries were produced without redactions on August 19, 2015, and the plaintiffs withdrew their motion as to those entries in a letter to the Court dated September 28, 2015.

b. The motion is moot with respect to entry 588 on Target's privilege log as Target has represented that it produced the corresponding email communication on October 19, 2014.

c. The motion is moot with respect to entries 744–45 on Target's privilege log as Target has represented that it produced the corresponding email communication on October 19, 2014.

d. The email communication corresponding to entry 89 on Target's privilege log is protected by the attorney-client privilege.

e. The email communications corresponding to entries 172–82 on Target's privilege log are protected by the attorney-client privilege and the work-product doctrine. In particular, Target has demonstrated, through the Declaration of Timothy Baer (Baer Decl. ¶¶ 8–9), that the work of the Data Breach Task Force was focused not on remediation of the breach, as Plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation that was already pending and was reasonably expected to follow. *See Rabushka v. Crane Co.*, 122 F.3d 559, 565 (8th Cir. 1997) (finding the non-movant on a motion to compel met its burden to establish work product and attorney-client privileges).

f. The email communications corresponding to entries 513–16 on Target's privilege log are protected by the attorney-client privilege. The

communications are between a Target in-house attorney and his clients and were made for the purpose of obtaining legal advice.

g. The email communications corresponding to entries 589–90 on Target's privilege log are protected by the work-product doctrine. Plaintiffs have not carried their burden to demonstrate that they have a substantial need for these materials to prepare their case, nor that they cannot, without undue hardship, obtain the substantial equivalent by other means. Fed. R. Civ. P. 26(b)(3)(A)(ii); *St. Paul Reinsurance Co, Ltd. v. Commercial Fin. Corp.*, 197 F.R.D. 620, 628 (N.D. Iowa 2000) (providing that the party seeking disclosure of information protected by work-product doctrine bears the burden of proving substantial need and undue hardship to obtain the materials once proponent of the protection meets its initial burden). Plaintiffs have not demonstrated that without these work-product protected materials they have been deprived of any information about how the breach occurred or how Target conducted its non-privileged or work-product protected investigation. Target has produced documents and other tangible things, including forensic images, from which Plaintiffs can learn how the data breach occurred and about Target's response to the breach. (*See* Visser Decl. ¶ 11, Ex. 7 (report prepared by a separate team from Verizon Business Network Services that was not engaged by Target's counsel and that conducted an investigation on behalf of several credit card issuing companies).)

h. The email communications corresponding to entries 746–49 on Target's privilege log are protected by the attorney-client privilege and work-

product doctrine. The communications are between a Target in-house attorney and his clients and were made for the purpose of obtaining legal advice and made in anticipation of litigation.

i. The email communications corresponding to entries 2004–05 on Target's privilege log are protected by the attorney-client privilege as Target has demonstrated the information in those communications was transmitted for the purpose of obtaining legal advice regarding the data breach investigation.

Date: October 23, 2015

s/ Jeffrey J. Keyes
JEFFREY J. KEYES
United States Magistrate Judge