American University Law Review

Volume 66 | Issue 5 Article 3

2017

Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach

Lawrence J. Trautman
Western Carolina University

Peter C. Ormerod
Western Carolina University

Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach

Abstract

On September 22, 2016, Yahoo! Inc. ("Yahoo") announced that a data breach and theft of information from over 500 million user accounts had taken place during 2014, marking the largest data breach ever at the time. The information stolen likely included names, birthdays, telephone numbers, email addresses, hashed passwords, and, in some cases, encrypted or unencrypted security questions and answers. Yahoo further disclosed its belief that the stolen data "did not include unprotected passwords, payment card data, or bank account information." Just two months before Yahoo disclosed its 2014 data breach, it announced a proposed sale of the company's core business to Verizon Communications. Then, during mid-December 2016, Yahoo announced that another 1 billion customer accounts had been compromised during 2013, a new record for largest data breach.

Social media and electronic commerce websites face significant risk factors, and an acquirer may inherit cyber liability and vulnerabilities. The fact pattern in this announced acquisition raises a number of important corporate governance issues: whether Yahoo's conduct leading up to the data breaches and its subsequent conduct constituted a breach of the duty to shareholders to provide security, the duty to monitor, the duty to disclose, or some combination thereof the impact on Verizon shareholders of the acquisition price renegotiation and Verizon's assumption of post-closing cyber liabilities; and whether more drastic compensation clawbacks for key Yahoo executives would be appropriate. Cybersecurity remains a threat to all enterprises, and this Article contributes to the corporate governance literature, particularly as it applies to mergers and acquisitions and the management of cyber liability risk.

CORPORATE DIRECTORS' AND OFFICERS' CYBERSECURITY STANDARD OF CARE: THE YAHOO DATA BREACH

LAWRENCE J. TRAUTMAN* AND PETER C. ORMEROD**

On September 22, 2016, Yahoo! Inc. ("Yahoo") announced that a data breach and theft of information from over 500 million user accounts had taken place during 2014, marking the largest data breach ever at the time. The information stolen likely included names, birthdays, telephone numbers, email addresses, hashed passwords, and, in some cases, encrypted or unencrypted security questions and answers. Yahoo further disclosed its belief that the stolen data "did not include unprotected passwords, payment card data, or bank account information." Just two months before Yahoo disclosed its 2014 data breach, it announced a proposed sale of the company's core business to Verizon Communications. Then, during mid-December 2016, Yahoo announced that another 1 billion customer accounts had been compromised during 2013, a new record for largest data breach.

Social media and electronic commerce websites face significant risk factors, and an acquirer may inherit cyber liability and vulnerabilities. The fact pattern in this announced acquisition raises a number of important corporate governance issues: whether Yahoo's conduct leading up to the data breaches and its subsequent conduct constituted a breach of the duty to shareholders to provide security, the duty to monitor, the duty to disclose, or some combination thereof; the impact on Verizon shareholders of the acquisition price renegotiation and Verizon's assumption of post-closing cyber liabilities; and whether more drastic compensation clawbacks for key Yahoo executives would be appropriate.

---

* Assistant Professor of Business Law and Ethics, *Western Carolina University.* JD, *Oklahoma City University School of Law*; MBA, *The George Washington University*; BA, *American University.* Mr. Trautman may be contacted at Lawrence.J.Trautman@gmail.com.

** Professor of Constitutional Law and Business Law, *Western Carolina University.* JD, *The George Washington University Law School*; BA, *The George Washington University, magna cum laude.* Mr. Ormerod may be contacted at ormerod.peter@gmail.com.

Cybersecurity remains a threat to all enterprises, and this Article contributes to the corporate governance literature, particularly as it applies to mergers and acquisitions and the management of cyber liability risk.

TABLE OF CONTENTS

INTRODUCTION

Yahoo! Inc. ("Yahoo" or the "Company") announced on September 22, 2016, that a state-sponsored hacker had breached the Company's digital systems in 2014 and had stolen personal information from over 500 million user accounts.[1] The information stolen likely included names, birthdays, telephone numbers, email addresses, "hashed passwords (the vast majority with bcrypt), and, in some cases, encrypted or unencrypted security questions and answers."[2] At the time it was announced, this 2014 theft represented the largest data breach ever.[3] This record would only later be surpassed by another Yahoo breach: a 2013 breach affecting 1 billion user accounts that the Company announced in December 2016.[4] Yahoo further disclosed its belief that the stolen data "did not include unprotected passwords, payment card data, or bank account information."[5] Just two months before Yahoo disclosed its 2014 data breach, it announced a proposed sale of the Company's core business to Verizon Communications, Inc. ("Verizon").[6] During mid-

1. *An Important Message to Yahoo Users on Security*, YAHOO! INC. (Sept. 22, 2016) [hereinafter *Yahoo Press Release*], https://finance.yahoo.com/news/important-message-yahoo-users-security-182800027.html.

2. *Id.*

3. *See* Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

4. *See* Robert McMillan, Ryan Knutson & Deepa Seetharaman, *Yahoo Discloses New Breach of 1 Billion User Accounts*, WALL ST. J. (Dec. 15, 2016, 5:19 PM), https://www.wsj.com/articles/yahoo-discloses-new-breach-of-1-billion-user-accounts-1481753131.

5. *Yahoo Press Release*, *supra* note 1.

6. *See Verizon to Acquire Yahoo's Operating Business*, PR NEWSWIRE (July 25, 2016, 7:00 AM), http://www.prnewswire.com/news-releases/verizon-to-acquire-yahoos-operating-business-300303133.html. Verizon emerged from the historic 1998 merger between Bell Atlantic Corp. and GTE Corp. on June 30, 2000. VERIZON, THE HISTORY OF VERIZON COMMUNICATIONS 1 (2016), http://www.verizon.com/about/sites/default/files/Verizon_History_0916.pdf. With approximately 177,700 employees and annual revenues exceeding $131 billion, Verizon is now one of the world's leading communications providers. VERIZON, 2015 ANNUAL REPORT 2, 10 (2016), https://www.verizon.com/about/sites/default/files/annual/verizon-annual-2015/downloads/15_vz_ar.pdf. Verizon Wireless, a Verizon subsidiary and the largest wireless service provider in the United States, has 112.1 million retail connections and accounts for approximately 70% of Verizon's total revenues. Verizon Communications, Inc., Annual Report (Form 10-K), at 2–3 (Feb. 23, 2016), https://www.sec.gov/Archives/edgar/data/732712/000119312516473367/d35513d10k.htm#tx35513_1. With 100% ownership over Verizon Wireless, Verizon is able to reach 98% of the U.S. population, equal to approximately 312 million Americans. VERIZON, 2015 ANNUAL REPORT, *supra*, at 10, 11.

December 2016, Yahoo announced that another 1 billion customer accounts had been compromised during 2013, establishing a new record for the largest data breach ever.

Almost all corporations—from technology companies like Yahoo to brick-and-mortar sales companies that use electronic commerce services—face a significant risk from data breaches, and mergers and acquisitions may result in cyber liability and vulnerabilities for the acquirer.[7] This announced acquisition raises a number of important corporate governance issues: whether Yahoo breached its duty to provide data security, its duty to monitor, its duty to disclose, or some combination thereof; the impact on Verizon shareholders of a renegotiated deal for the two companies to share the cost of liability; and whether more severe and wide-ranging compensation clawbacks would be appropriate.

This Article proceeds in three parts. Part I discusses corporate governance and the director's duty of care, including the duty to secure data and the duties to monitor and disclose. Part II presents a brief description of Yahoo; outlines Verizon's proposed acquisition; describes the Yahoo data breaches and their known impact to date; and looks at Yahoo's executive compensation, code of ethics, and duty to disclose material events. Part III examines the important corporate governance issues raised by the proposed Yahoo/Verizon transaction. The Article concludes with some thoughts on the evolution of corporate liability as it relates to data security and what the future may hold for this important and fast-developing area of the law.

I. CORPORATE GOVERNANCE AND THE DIRECTOR'S DUTY OF CARE

A. The Duty to Provide Data Security

Corporate directors and officers have a duty to behave reasonably. This duty of care applies across directors' and officers' myriad responsibilities, including handling the corporation's digital data. There is, therefore, an emerging specific application of the duty of care as related to information technology: the duty to secure data. The applicable standard of care requires directors "to provide 'reasonable' or 'appropriate' physical, technical, and administrative

7. *See* Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230, 240 (2016) (discussing the risk assumed by companies that acquired malware-tainted Nortel software from bankruptcy proceeding); *see also* Lawrence J. Trautman & George P. Michaely, Jr., *The SEC & the Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. 262 (2014) (discussing electronic commerce operations and websites).

security measures to ensure the confidentiality, integrity, and availability of corporate data."[8]

There is not, however, a single source—such as a comprehensive federal statute or regulation—that imposes a duty to provide data security. Rather, corporate legal obligations to implement data security systems are "set forth in an ever-expanding patchwork of state, federal, and international laws, regulations, and enforcement actions, as well as in common law duties, contractual commitments, and other expressed and implied obligations to provide 'reasonable' or 'appropriate' security for corporate data."[9]

1. Sources of the duty

a. Statutes and regulations

The primary statutory and regulatory sources of corporate data security obligations are diverse: privacy laws, data security laws, electronic transaction laws, corporate governance laws, unfair and deceptive business practice and consumer protection laws, and breach notification laws.[10]

There are several federal privacy statutes—paired with implementing regulations—that require corporations to create and maintain information security systems to protect specific types of personal data about individuals. Particularly important examples include the Financial Services Modernization Act of 1999,[11] which concerns the financial sector; the Health Insurance Portability and

8. THOMAS J. SMEDINGHOFF, INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE 29 (2008).

9. *Id.*; *see also* Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works*, 5 J.L. & CYBER WARFARE 147 (2016); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341; Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COMM. L.J. 205 (2013); Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire*, 8 J. STRATEGIC & INT'L STUD. 105 (2013).

10. *See* Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors 4–6 (Oct. 8, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323; *see also* SMEDINGHOFF, *supra* note 8, at 30–31.

11. Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999 ("GLBA"), Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 and 15 U.S.C.). *See generally* Timothy J. Yeager, Fred C. Yeager & Ellen Harshman, *The Financial Services Modernization Act: Evolution or Revolution?*, 59 J. ECON. & BUS. 313 (2007).

Accountability Act of 1996,[12] which concerns healthcare information; the Privacy Act of 1974,[13] which establishes governmental record-keeping requirements; and the Children's Online Privacy Protection Act,[14] which applies to all businesses that collect personal information on the Internet from children.

Additionally, several states—including Arkansas, California, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah—have enacted data security statutes that impose "a general obligation on all companies to ensure the security of personal information."[15] For example, California, which was the first state to enact this type of legislation in 2004, requires all businesses to "implement and maintain reasonable security procedures and practices" to protect California residents' personal information against "unauthorized access, destruction, use, modification, or disclosure."[16] Further, several federal regulations impose a duty to protect specific types of information, such as IRS revenue procedures requiring security measures to protect electronic tax records[17] and SEC regulations requiring the protection of corporate financial data.[18]

Some electronic transactions laws and implementing regulations intended to maintain the fidelity, accuracy, and enforceability of electronic documents also require data security for electronic record-keeping. The Electronic Signatures in Global and National Commerce Act is the guiding federal statute, whereas the Uniform Electronic Transactions Act applies at the state level.[19] Both mandate companies secure electronic records that relate to online transactions, primarily through requirements concerning the data's accessibility, integrity, and accuracy.[20]

From a corporate governance perspective, several statutes and implementing regulations are designed to protect public companies' shareholders, investors, and business partners. The two chief sources of authority from which corporate governance data security

12. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 and 42 U.S.C.).

13. Privacy Act of 1974, 5 U.S.C. § 552a (2012).

14. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–02 (2012).

15. Smedinghoff, *supra* note 10, at 5.

16. CAL. CIV. CODE § 1798.81.5(b) (West 2016); *see also* Smedinghoff, *supra* note 10, at 5.

17. *See* Rev. Proc. 97-22, 1997-1 C.B. 652; Rev. Proc. 98-25, 1998-1 C.B. 689.

18. *See* 17 C.F.R. §§ 240.17a-4, 248.30 (2015); 17 C.F.R. § 257.1(e)(3) (2011).

19. UNIF. ELEC. TRANSACTIONS ACT ("UETA") § 7 (UNIF. LAW COMM'N 1999).

20. *See id.* § 12; *see also* E-SIGN, 15 U.S.C. § 7001(d)–(e) (2012) (clarifying that statutory requirements to retain documents or to execute documents in writing are satisfied by electronic documents so long as the electronic versions are accurate and accessible).

obligations flow are the Sarbanes-Oxley Act[21] and the SEC's 2011 guidance.[22] The Sarbanes-Oxley Act requires public companies to implement appropriate information security controls regarding companies' financial information.[23] The SEC's 2011 guidance identifies risks to cybersecurity as potential material information that companies must disclose under pre-existing securities law disclosure requirements and accounting standards.[24]

Among unfair and deceptive business practice and consumer protection laws, section 5 of the Federal Trade Commission Act (FTC Act),[25] associated Federal Trade Commission (FTC) enforcement actions, and equivalent state statutes are the chief sources for the imposition of data security obligations. Between 2002 and 2005, the FTC and equivalent state entities brought cybersecurity-related enforcement actions premised on a deceptive trade practice theory of liability: companies were liable for failing to provide adequate information security, contrary to the representations they made to consumers.[26] The parties resolved these actions by entering into consent decrees wherein corporations agreed to take affirmative steps to better protect information in their systems.[27]

---

21. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 11, 15, 18, 28, and 29 U.S.C.).

22. *Corporate Finance Disclosure Guidance: Topic No. 2: Cybersecurity*, DIV. OF CORP. FIN., U.S. SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [hereinafter *SEC CF Disclosure Guidance*].

23. Bruce H. Nearon et al., *Life After Sarbanes-Oxley: The Merger of Information Security and Accountability*, 45 JURIMETRICS 379, 391, 394 (2005).

24. *SEC CF Disclosure Guidance*, *supra* note 22 (explaining that federal law requires a company to disclose particularized risks specific to the company, not boilerplate or generic risks that could apply to any firm in the industry).

25. 15 U.S.C. § 45.

26. *See, e.g.*, Compl. ¶¶ 12–16, *In re* Guess?, Inc., File No. 022 3260, 2003 WL 21406017 (F.T.C. June 18, 2003) (arguing that it is a deceptive trade practice to represent to consumers, through a published privacy policy and answers to "frequently asked questions," that consumer personal information is encrypted when a commonly used method of cyberattack could obtain this information in clear, unencrypted text); Compl. ¶¶ 12–14, *In re* MTS, Inc., 032-3209, 2004 WL 963226 (F.T.C. Apr. 21,. 2004) (claiming that the failure to use an "authentication code" in the new ordering system allowed a vulnerability and therefore access to private consumer information in contravention of the company's published Privacy Policy, which amounted to a deceptive trade practice).

27. *See, e.g.*, Agreement Containing Consent Order at secs. II, V, *In re* Guess?, Inc., File No. 022 3260 (F.T.C. June 18, 2003), www.ftc.gov/os/2003/06/guessagree.htm (ordering a corporation to implement safeguards sufficient for its size and complexity by designating employees to work on cyber security, conducting a risk assessment, tailoring safeguards to any particularized risks discovered, and changing business practices to conform with the

But after 2005, the FTC significantly broadened the scope of its cybersecurity-related enforcement actions by contending that a company's failure to provide appropriate data security for consumers' personal information was, alone, an *unfair* trade practice; that is, a company could be liable without ever having misrepresented the extent of its data security practices to consumers.[28] Subsequently, in August 2015, the Third Circuit ratified the FTC's broader theory of liability.[29]

To date, forty-seven states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have also enacted cybersecurity breach notification laws, which impose an obligation to disclose security breaches to those affected.[30] Myriad federal banking regulations also impose an obligation on financial institutions to disclose security breaches.[31]

---

new information security safeguards); Agreement Containing Consent Order at secs. II, V, *In re* MTS, Inc., File No. 032-3209 (F.T.C. Apr. 21, 2004), www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf (same).

28. *A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach: Hearing on Discussion Draft of H.R. ___ Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 44 (2011) (statement of Edith Ramirez, Comm'r, FTC) ("[T]he Commission enforces the FTC Act's proscription against unfair . . . acts . . . in cases where a business['s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury."); *The Threat of Data Theft to American Consumers: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 15 (2011) (statement of David Vladeck, Dir., Bureau of Consumer Prot., FTC) (same).

29. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 245–47, 249, 259 (3d Cir. 2015) (holding that Wyndham's failure to secure consumer information, which resulted in actual harm to consumers, fell within the plain meaning of "unfair"). *See generally* Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1209–12 (2017) (describing how the FTC's section 5 enforcement authority applies to companies' cybersecurity policies).

30. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATORS (Feb. 24, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

31. Supplement A to Appendix B to Part 30-Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. § 30 (OCC) (providing guidance to financial institutions about what the consumer notice of breach should include); Supplement A to Appendix D-2 to Part 208-Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice, 12 C.F.R. § 208 (Federal Reserve System), Supplement A to Appendix B to Part 364-Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 C.F.R. § 364 (FDIC); 12 C.F.R. § 568.5 (Office of Thrift Supervision); *see also* Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice, 70 Fed. Reg. 15,736, (Mar. 29, 2005) (to be codified at 12 C.F.R. pts. 30, 208, 225, 364, 568 & 570) (reviewing commentator feedback on agency proposed guidance for how institutions should respond and notify consumers following unauthorized access to consumer information).

b. Federal executive branch action

Federal executive action also serves a function in data security. In February 2013, President Obama issued an executive order that, in part, "expanded public-private information sharing and tasked the [National Institute for Standards and Technology ('NIST')] with establishing a voluntary 'Cybersecurity Framework' comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure."[32] While there have been critics on both sides of the new NIST Cybersecurity Framework—some argue it does not go far enough, while others contend the framework is hardly "voluntary"—it nonetheless "has the potential to shape a standard of care for domestic critical infrastructure organizations."[33] Not only that, but some commentators are hopeful that, particularly for corporations like Yahoo that operate across jurisdictions, "a global standard of cybersecurity care could eventually emerge [organically] that would promote consistency and contribute to 'cyber peace' even absent regulatory action."[34]

On May 11, 2017, President Trump signed an executive order intended to improve the federal government's cybersecurity and protect critical infrastructure from digital attacks.[35] The most notable changes include requiring "heads of federal agencies [to] use a framework developed by the National Institute of Standards and Technology to assess and manage cyber risk, and prepare a report within 90 days documenting how they will implement it."[36]

c. Common law

Scholars and commentators have long contended there is a common law duty to provide adequate security for corporate data.[37]

---

32. Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 308 (2015).

33. *Id.* at 308–10.

34. *Id.* at 311; *see also* Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?*, 18 N.C. J.L. & TECH. 233, 236 (2016) (hypothesizing a large-scale cyberattack and its fallout to illustrate the necessity for a global standard for cybersecurity).

35. Dustin Volz, *Trump Signs Order Aimed at Upgrading Government Cyber Defenses*, REUTERS (May 11, 2017, 5:11 PM), http://www.reuters.com/article/us-usa-trump-cyber-idUSKBN1872L9.

36. *Id.*

37. SMEDINGHOFF, *supra* note 8, at 31 (citing Kimberly Krefer & Randy V. Sabett, *Openness of Internet Creates Potential for Corporate Information Security Liability*, Elec. Commerce & Law Rep. (BNA), Vol. 7, No. 24, at 594 (June 12, 2002); Alan Charles Raul et al., *Liability for Computer Glitches and Online Security Lapses*, Elec. Commerce &

While at least one court has explicitly held there is no corporate duty to provide security,[38] several courts have concluded just the opposite. In 2005, for instance, a state appellate court in *Bell v. Michigan Council 25*[39] held that the "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information."[40]

And, more recently, a federal district court held,

> Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. . . . As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.[41]

d. Contractual obligations

In situations where third parties have possession of, control over, or access to corporate data, companies that entrust third parties to manage their data are increasingly trying to satisfy their duty to protect the security of their data by contract.[42] For example, some companies contract for "cloud computing" services, in which a third party is charged with storing and processing a company's data.[43]

Law Rep. (BNA), Vol. 6, No. 31, at 849 (Aug. 8, 2001); Erin Kenneally, *The Byte Stops Here: Duty and Liability for Negligent Internet Security*, XVI COMPUTER SECURITY J. (2000)).

38. Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 30 (Ill. App. Ct. 2010) (finding that the Consumer Fraud Act only restricted "persons" from publicly posting an individual's private information, and the School Board was not a "person," thus rejecting an independent duty to safeguard private information).

39. No. 246684, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005) (per curiam).

40. *Id.* at *5.

41. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966, (S.D. Cal. 2014) (citations omitted); *see also* Lawrence J. Trautman, The SONY Data Hack: Implications for World Order (unpublished manuscript).

42. Smedinghoff, *supra* note 10, at 8.

43. *Id.* (adding that, similarly, access to a trading partner's data often comes with contractual security obligations). A similar example involving multiple parties is the Payment Card Industry Data Security Standard ("PCI Standard"). Merchants that want to accept credit credits at the point of sale must contractually agree to compliance with the PCI Standard. PAYMENT CARD INDUSTRY SECURITY STANDARDS

These contracts shift the data security duty from the contracting company to the cloud computing company through cyber liability indemnification provisions.

e. Self-imposed obligations

Finally, companies increasingly impose security obligations on themselves. As noted above, the FTC has aggressively pursued deceptive trade practice enforcement actions against companies that make representations in privacy policies, on websites, or in advertising materials that are inconsistent with the entity's actual data security practices.[44]

2. The standard of care for the duty

Of the authorities discussed above that impose a data security duty, most simply state that there is "an obligation to implement 'reasonable' or 'appropriate' security measures," but they "provide little or no guidance as to what is required for legal compliance."[45] While there is little question that the legal standard for what constitutes reasonable security is still emerging, much progress has been made in recent years.

Thomas J. Smedinghoff, a leading expert on this emerging cybersecurity standard, explains that the emerging digital security standard is particularized and case specific.[46] Unlike prior specific requirements, such as passwords or firewalls, the new corporate security obligation is fact-specific, requiring companies to go through a "process" and determine what security measures are most appropriate for the company's security needs.[47] The emerging legal standard follows suit by allowing companies to create their own specific security measures so long as the companies conduct ongoing reviews of their security mechanisms.[48] This repetitive review process includes detecting and evaluating risks, implementing specific security responses to those risks, verifying the effective

---

COUNCIL, VERSION 3.2, DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES 5 (2016); Smedinghoff, *supra* note 10, at 8.

44. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014) (holding that in light of Wyndham's publication of a privacy policy, in which it promised to protect consumers' personal information, the failure to implement corresponding security measures amounted to an unfair practice under the FTC Act), *aff'd*, 799 F.3d 236, 241, 259 (3d Cir. 2015).

45. Smedinghoff, *supra* note 10, at 9.

46. *Id.* at 9–10.

47. *Id.*

48. *Id.*

implementation of those security responses, and updating the measures as needed in reaction to developing security concerns.[49]

Specifically, Mr. Smedinghoff's process-oriented approach to satisfying a "reasonable" or "appropriate" standard of care for a duty to provide security is composed of the following seven provisions[50]:

Assign Responsibility: A corporation should expressly designate one or more employees to be responsible for maintaining the data security program.

Identify Information Assets: A corporation should identify its information assets that require protection, which include both the data itself (i.e., records containing personal information) and the computing systems that store the personal information (e.g., servers, laptops, and portable devices).

Conduct Risk Assessment: A corporation should perform a risk assessment to identify both internal and external risks to its data security, and it should evaluate the effectiveness of the company's current practices for safeguarding and minimizing the risks identified.

Select and Implement Responsive Security Controls: A corporation should implement physical, administrative, and technical security controls it considers appropriate to minimize the risks it identified in its risk assessment.

Monitor Effectiveness: A corporation should *regularly* monitor, test, and reassess the security controls it has chosen to implement in order to ensure its security program is operating in a manner reasonably calculated to protect personal information. Relatedly, a corporation should regularly upgrade its security controls as necessary to limit emerging risks.

Regularly Review the Security Program: A corporation should review and adjust its data security program no less than once per year. A corporation should also perform security program reviews whenever there is a material change in business practices that could affect personal information or after any incident involving a breach of its data security.

Address Third Party Issues: A corporation should take all reasonable steps to verify that every third-party service provider that has access to the company's data assets and personal information has the capacity to protect that information.[51]

An ever-increasing number of authorities are expressly adopting this process-oriented approach to data security, which is referred to as

---

49. *Id.*
50. *Id.* at 10.
51. *Id.*

a Written Information Security Program ("WISP").[52] The FTC is the most important of the authorities that have adopted the WISP standard. According to the FTC, businesses in all industries should comply with the process-oriented approach to information security as it demonstrates the "best practice" for legal compliance.[53] The FTC has demonstrated this view by requiring any company resolving FTC complaints about failure to provide adequate information security through consent decrees to implement and comply with this process-oriented approach.[54] The FTC's adherence to the WISP standard is particularly important in light of the agency's post-2005 theory of liability that sanctions a duty to protect data.[55]

3. The FTC's cybersecurity unfair trade practices theory of liability

As noted briefly above, since 2005, the FTC has pursued administrative actions against companies "with allegedly deficient cybersecurity that failed to protect consumer data against hackers"[56] under the FTC Act's provision that prohibits "unfair . . . acts or practices in or affecting commerce."[57] Commentators have analogized the jurisprudence that these FTC actions has spawned to an authoritative body of common law that operates in lieu of comprehensive cybersecurity legislation.[58] Professors Daniel J. Solove and Woodrow Hartzog explain,

> [A] deeper look at the principles that emerge from FTC privacy "common law" demonstrates that the FTC's privacy jurisprudence is quite thick. The FTC has codified certain norms and best

52. *See, e.g.*, 201 MASS. CODE REGS. § 17.03 (2017); HIPAA Security Standards, 45 C.F.R. § 164.308 (2017). *See generally* Bruce Radke & Michael J. Waters, *Selected State Laws Governing the Safeguarding and Disposing of Personal Information*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 487 (2015) (comparing different state WISP regulations).

53. Smedinghoff, *supra* note 10, at 11 (citing *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Tech. & Homeland Sec. of the S. Comm. on the Judiciary*, 110th Cong. 7, 93 (statement of Lydia Parnes, Dir., Bureau of Consumer Prot., FTC)) (remarking that "'the FTC Safeguards Rule promulgated under the GLB Act serves as a good model' for satisfying the obligation to maintain reasonable and appropriate security").

54. *Id.*

55. *See, e.g.*, Brad Lunn, *Strengthened Director Duties of Care for Cybersecurity Oversight: Evolving Expectations of Existing Legal Doctrine*, 4 J.L. & CYBER WARFARE 109, 124, 127 (2014) (describing the duty to protect in the context of the responsibilities of company director to be informed and actively engaged in cybersecurity issues that arise in a company).

56. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

57. 15 U.S.C. § 45(a)(1) (2012).

58. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 604–05, 619–20 (2014).

> practices and has developed some baseline privacy protections. Standards have become so specific they resemble rules. The FTC has thus developed a surprisingly rich jurisprudence. We contend that the foundations exist to develop this "common law" into a robust privacy regulatory regime, one that focuses on consumer expectations of privacy, extends far beyond privacy policies, and involves a full suite of substantive rules that exist independently from a company's privacy representations.[59]

An additional contributor to this body of law's scant level of scholarly analysis is the fact that "[t]he vast majority of [FTC cyber liability] cases have ended in settlement."[60] But this may be changing: the U.S. Court of Appeals for the Third Circuit specifically affirmed the FTC's theory of liability under the unfairness prong in August 2015.[61] The Third Circuit's *FTC v. Wyndham Worldwide Corp.* case was a rare exception where a court opined on the FTC's cybersecurity liability strategy.[62] Because it is inevitable the FTC will bring an administrative action against Yahoo for the 2014 data breach, a closer examination of the Third Circuit's decision in *Wyndham* follows.

In 2008 and 2009, hackers breached Wyndham Worldwide Corporation's computer systems three times, stealing hundreds of thousands of customers' personal and financial information, which resulted in over $10.6 million in fraudulent charges.[63] As a result, the FTC filed suit in U.S. district court under 15 U.S.C § 45(a), alleging, inter alia, that Wyndham's failure to provide adequate protection for private customer information was an unfair trade practice.[64] After the district court denied Wyndham's motion to dismiss the complaint, the Third Circuit granted an interlocutory appeal to address "whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that

---

59. *Id.* at 586.

60. *Wyndham Worldwide Corp.*, 799 F.3d at 240.

61. *Id.* at 240, 247.

62. Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator:* FTC v. Wyndham *and Its Implications*, Privacy & Sec. L. Rep. (BNA), Vol. 13, at 621 (Apr. 14, 2014) (explaining that the court's rare opportunity to comment arose because Wyndham was the first company unwilling to settle the FTC's complaint). For a decade, the FTC alleged that deficient information security amounted to an unfair trade practice, and every complaint it filed during this decade settled. *Id.*

63. *Wyndham*, 799 F.3d at 240.

64. *Id.*

provision."[65] The Third Circuit affirmed the district court and ruled in the FTC's favor on both questions.[66]

Addressing the first issue, the Third Circuit reviewed in detail the FTC Act's legislative history and the FTC's past practices, and it noted that both flexibility and ambiguity were purposefully built into the Act.[67] Accordingly, the court dismissed Wyndham's argument that its cybersecurity practices "[fell] outside the plain meaning of 'unfair.'"[68] Among other arguments Wyndham raised, it asserted that the corporation could not treat its customers in an unfair manner when criminal hackers victimize the corporation too.[69] The court rejected the argument, pointedly noting that "[a]lthough unfairness claims 'usually involve actual and completed harms,' 'they may also be brought on the basis of likely rather than actual injury,'"[70] particularly because the FTC Act "expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[71]

B. The Duty to Monitor

Among other duties, corporate directors and officers owe the corporation and its shareholders a duty of care. The duty of care is a concept adapted from tort law, and it requires an actor to behave reasonably.[72] Director liability for a breach of the duty of care may arise in two distinct contexts.[73] First, liability may "follow from a board decision that results in a loss because that decision was ill advised or 'negligent.'"[74] Second, liability may "arise from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss."[75]

---

65. *Id.*

66. *Id.* at 259.

67. *Id.* at 243 (citing FTC v. Bunte Bros., 312 U.S. 349, 353 (1941) (contrasting unfair competition with the rather clear-cut problem of rate discrimination)).

68. *Id.* at 247.

69. *Id.* at 246.

70. *Id.* (quoting *In re* Int'l Harvester Co., 104 F.T.C. 949, 1061 & n.45 (1984)).

71. *Id.* (citing 15 U.S.C. § 45(n) ("[An unfair act or practice] causes or is likely to cause substantial injury.")).

72. Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139, 1159–60 (2013).

73. *See In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996).

74. *Id.*

75. *Id.* (citing E. Norman Veasey & Julie M.S. Seitz, *The Business Judgment Rule in the Revised Model Act, the* Trans Union *Case, and the ALI Project—A Strange Porridge*, 63 TEX. L. REV. 1483 (1985)).

In *In re Caremark International Inc. Derivative Litigation*,[76] a seminal 1996 Delaware Chancery Court decision on the duty of care, the court took pains to emphasize that judicial inquiries into a director's affirmative actions center on the adequacy of the *process* that gave rise to the shareholders' derivative action, not the *content* of the decision itself.[77] Therefore, a director will not be found liable for a decision after-the-fact if the decision making process used was in good faith or rational in promoting the corporation's interest.[78] The overwhelming majority of a director's affirmative acts are evaluated under the deferential business judgment rule. But the business judgment rule applies differently in situations where a director's lax oversight—a failure to monitor and be informed—results in corporate losses.[79]

At its core, a breach of the duty to monitor arises when "a loss eventuates not from a decision but, from unconsidered inaction."[80] Noting that "[m]ost of the decisions that a corporation, acting through its human agents, makes are . . . not the subject of director attention," the *Caremark* court nonetheless recognized that "ordinary business decisions that are made by officers and employees deeper in the interior of the organization can . . . vitally affect the welfare of the corporation and its ability to achieve its various strategic and financial goals."[81]

At a minimum, corporate boards fail to satisfy their obligation to be reasonably informed about the corporation if they do not "assur[e] themselves that information and reporting systems exist in the organization that are reasonably designed to provide . . . timely, accurate information sufficient to allow management and the board . . . to reach informed judgments concerning . . . the corporation's compliance with law."[82] This is not to say, however, that there is a universal, one-size-fits-all solution to the duty to monitor—"the level of detail that is appropriate for such an information system is a question of business judgment."[83] Nor does the existence of an adequate monitoring system eliminate the risk "that the corporation will violate laws or regulations, or that senior officers or directors may

---

76. 698 A.2d 959 (Del. Ch. 1996).

77. *Id.* at 967.

78. *Id.* (explaining that applying an "objective" standard during judicial review would "expose directors to substantive second guessing by ill-equipped judges or juries, which would . . . be injurious to investor interests").

79. *See* Veasey & Seitz, *supra* note 75, at 1502.

80. *Caremark*, 698 A.2d at 968.

81. *Id.*

82. *Id.* at 970.

83. *Id.*

nevertheless sometimes be misled or otherwise fail reasonably to detect acts material to the corporation's compliance with the law."[84]

Thus, the duty to monitor requires "the board [to] exercise a good faith judgment that the corporation's information and reporting system is in *concept and design* adequate to assure the board that appropriate information will come to its attention in a timely manner."[85] To avoid liability and conform to relevant legal norms, a director should attempt in good faith to ensure the company has a "corporate information and reporting system" that the board finds satisfactory.[86] Accordingly, the corporate law duty of care centers on whether corporate directors and officers employed a "good faith effort" to remain reasonably informed sufficient to "exercise good judgment."[87]

C. The Duty to Disclose

A publicly traded corporation's duty to disclose the existence of a data breach stems from at least two distinct authorities: Delaware state corporate common law and the SEC's 2011 corporate finance disclosure guidance, which identifies material data security risks that companies must disclose under securities law disclosure requirements and accounting standards.[88] Companies that know about a data breach but fail to disclose it to shareholders, regulators, and consumers risk liability under potentially corporate, breach notification, and securities laws.

---

84. *Id.*

85. *Id.* (emphasis added).

86. *Id.* at 968.

87. *Id.*; *see also* William T. Allen et al., *Realigning the Standard of Review of Director Due Care with Delaware Public Policy: A Critique of* Van Gorkom *and Its Progeny as a Standard of Review Problem*, 96 NW. U. L. REV. 449, 457 & n.31 (2002) (stating that directors "will not be held liable" for a breach of the duty to monitor without a finding of bad faith); Christopher M. Bruner, *Is the Corporate Director's Duty of Care a "Fiduciary" Duty? Does It Matter?*, 48 WAKE FOREST L. REV. 1027, 1047 (2013) (asserting that liability under the *Caremark* standard requires bad intention toward the company, such as "total board failure to engage in oversight"); Lynn A. Stout, *In Praise of Procedure: An Economic and Behavioral Defense of* Smith v. Van Gorkom *and the Business Judgment Rule*, 96 NW. U. L. REV. 675, 680 (2002) (noting that in some states, directors are presumed to meet the duty of care if the decision was "informed," and "unless the directors [have been] *grossly* negligent in failing to inform themselves, before acting," the decision is deemed to be informed).

88. *See* Lawrence A. Hamermesh, *Calling off the* Lynch *Mob: The Corporate Director's Fiduciary Disclosure Duty*, 49 VAND. L. REV. 1087, 1089–91 (1996); *SEC CF Disclosure Guidance*, *supra* note 22.

Directors' and officers' fiduciary duty to shareholders and the corporation imposes a duty to disclose—sometimes referred to as a duty of complete candor—that is well established in Delaware common law.[89]

Two decades ago, Professor Lawrence A. Hamermesh noted that Delaware courts have recognized "that a fiduciary duty to disclose all material information arises when directors approve any public statement, such as a press release, regardless of whether any specific stockholder action is sought."[90] Director negligence is irrelevant in assessing the duty to disclose.[91] The duty serves two purposes: (1) to "afford stockholders a remedy," regardless of whether they relied upon a misstatement or omission, and (2) "to afford a 'virtual per se rule' of damages," awarding stockholders a monetary award "without having to establish actual loss."[92]

The Delaware Supreme Court later confirmed Professor Hamermesh's interpretation. In *Malone v. Brincat*,[93] the Delaware Supreme Court clarified that directors and officers owe a duty of honesty to shareholders in both communications seeking shareholder action and "[w]henever directors communicate publicly or directly with shareholders about the corporation's affairs, with or without a request for shareholder action."[94] The court held that "directors who knowingly disseminate false information that results in corporate injury or damage to an individual stockholder violate their fiduciary duty, and may be held accountable in a manner appropriate to the circumstances."[95] In sum, the duty to disclose in Delaware requires that directors provide shareholders with "all material information" about the corporation whenever they communicate with the shareholder or market, even if the shareholder did not request it.[96]

Additionally, the SEC's 2011 Guidance notes that "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."[97] Although the Guidance acknowledges that "no existing disclosure requirement explicitly refers to cybersecurity risks and

89. Hamermesh, *supra* note 88, at 1097 & nn.34–35.
90. *Id.* at 1091.
91. *Id.*
92. *Id.*
93. 722 A.2d 5 (Del. 1998).
94. *Id.* at 10.
95. *Id.* at 9.
96. Shannon German, *What They Don't Know Can Hurt Them: Corporate Officers' Duty of Candor to Directors*, 34 DEL. J. CORP. L. 221, 233 (2009).
97. *SEC CF Disclosure Guidance*, *supra* note 22.

cyber incidents," the SEC nonetheless required the disclosure of "material information regarding cybersecurity risks and cyber incidents" to prevent misleading the public.[98]

The Guidance provides examples of situations in which disclosure is mandatory—several of which are likely implicated here. First, the Guidance provides that the SEC "expect[s] 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.*"[99] Second, the Guidance advises that

> [r]egistrants should address cybersecurity risks and cyber incidents . . . 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.[100]

Consequently, some commentators—like Jacob Olcott, former Senate Commerce Committee counsel—believe that the "Yahoo hack could become a test case of the SEC's [2011] guidelines . . . due to the size of the breach, intense public scrutiny and uncertainty over the timing of Yahoo's discovery."[101]

II. YAHOO

A. Background

Founded in 1994 as *Jerry and Dave's Guide to the World Wide Web* by Stanford graduate students Jerry Yang and David Filo, Yahoo was incorporated under the laws of the State of Delaware in 1995.[102] Headquartered in Sunnyvale, California, milestones in Yahoo's corporate growth include completion of an initial public offering on April 12, 1996, and subsequent listing under the ticker symbol "YHOO" on the NASDAQ Global Market.[103] Yahoo describes itself as "a guide to digital information discovery, focused on informing, connecting, and entertaining [its] users through [its] search, communications, and

98. *Id.*

99. *Id.* (emphasis added).

100. *Id.*

101. *See* Dustin Volz, *Yahoo Hack May Become Test Case for SEC Data Breach Disclosure Rules*, REUTERS (Sept. 30, 2016, 5:24 PM), http://www.reuters.com/article/us-yahoo-cyber-disclosure-idUSKCN1202MG.

102. *See* Yahoo! Inc., Preliminary Proxy Statement (Schedule 14A) (Sept. 9, 2016) [hereinafter Preliminary Proxy Statement], https://www.sec.gov/Archives/edgar/data/1011006/000119312516706578/d206374dprem14a.htm.

103. *Id.*

digital content products. By creating highly personalized experiences, [Yahoo] help[s] users discover the information that matters most to them around the world—on mobile or desktop."[104]

For the fiscal year that ended December 31, 2015, Yahoo's revenue reached $4.96 billion, with search and display advertising accounting for 84 percent.[105] Accordingly, Yahoo articulates its value proposition for advertisers as consisting of "a streamlined, simple advertising technology stack that leverages Yahoo's data, content, and technology to connect advertisers with their target audiences," where "[a]dvertisers can build their businesses through advertisements targeted to audiences on [Yahoo's] online properties and services . . . and a distribution network of third-party entities."[106]

Social media and electronic commerce websites face significant competition and other risk factors.[107] Yahoo's significant competition includes that from "search engines, sites offering integrated internet products and services, social media and networking sites, ecommerce sites, companies providing analytics, monetization and marketing tools for mobile and desktop developers, and digital, broadcast and print media."[108] Yahoo also experiences substantial international competition from local service providers in the Latin America, Middle East, Asia, and European markets.[109]

Yahoo's approximate thirty-six percent ownership position in Yahoo Japan resulted from a 1996 joint venture agreement with SoftBank Group Corp. ("SoftBank").[110] In addition, on October 23, 2005, Yahoo acquired an approximate forty percent equity position (on a fully-diluted basis) in Alibaba, a Chinese e-commerce business, common stock in exchange for Yahoo's China-based businesses—a cash investment of $1 billion and $8 million in transaction costs.[111] Alibaba's core commerce enterprise in the People's Republic of China consists of two distinct marketplace operations: wholesale commerce

---

104. Yahoo! Inc., Annual Report (Form 10-K), at 4 (Feb. 29, 2016) [hereinafter Yahoo 2015 10-K], https://www.sec.gov/Archives/edgar/data/1011006/000119312516483790/d12894d10k.htm.

105. *Id.* at 13, 37.

106. *Id.* at 4.

107. *See* Lawrence J. Trautman, *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal*, 16 U.C. DAVIS BUS. L.J. 261, 264 (2016) (including as risk factors "credit cards; U.S. state money transmission laws; online and mobile growth; and reliance on internet access").

108. Yahoo 2015 10-K, *supra* note 104, at 12.

109. *Id.*

110. *See* Preliminary Proxy Statement, *supra* note 102, at 35.

111. *See id.* at 36.

and retail commerce.[112] Alibaba's third area of core commerce business consists of cross-border and international commerce.[113] Other significant Alibaba businesses include cloud computing, entertainment, mobile media, and other innovation initiatives.[114] A series of Alibaba transactions have been significant to Yahoo's fortunes during recent years: In 2012, Alibaba repurchased 523 million shares from Yahoo in exchange for $7.1 billion.[115] And in 2014, Yahoo sold 140 million shares during Alibaba's initial public offering for approximately $9.4 billion.[116] As of September 13, 2016, Yahoo retains an approximate fifteen percent interest in Alibaba outstanding ordinary shares,[117] valued at approximately $36.7 billion.[118]

Third quarter 2016 results for Yahoo showed continued deterioration in core advertising revenues, constituting the seventh decline in this key business metric during the past eight quarters.[119] Table 1 illustrates certain financial results for Yahoo during the fiscal years that ended December 31 for the periods 2013 through 2015, and it displays the following key financial metrics:

> [R]evenue; revenue less traffic acquisition costs ("TAC"), or revenue ex-TAC; income (loss) from operations; adjusted earnings before interest, tax, depreciation, and amortization ("EBITDA"); net income (loss) attributable to Yahoo! Inc.; net cash provided by (used in) operating activities; and free cash flow. Revenue ex-TAC, adjusted EBITDA, and free cash flow are financial measures that are not defined in accordance with U.S. generally accepted accounting principles ("GAAP"). These non-GAAP financial measures are helpful for internal managerial purposes and to facilitate period-to-period comparisons.[120]

---

112. *Id.* at 36.
113. *Id.*
114. *Id.*
115. *Id.*
116. *Id.*
117. *Id.*
118. Jen Wieczner, *Here's Why Alibaba Will Never Buy Back Yahoo Stake*, FORTUNE (Sept. 13, 2016), http://fortune.com/2016/09/13/alibaba-yahoo-stock.
119. *See* Deepa Seetharaman, *Yahoo Looks to Bright Side After Breach*, WALL ST. J. (Oct. 19, 2016), https://www.wsj.com/articles/yahoo-core-revenue-drops-again-1476822440.
120. *Id.*

Table 1: Yahoo Key Financial Metrics[121]

Financial Metric	Amount (in thousands of dollars) for Years Ended December 31		
	2013	*2014*	*2015*
Revenue	4,680,380	4,618,133	4,968,301
Revenue ex-TAC	4,425,938	4,400,602	4,090,787
Income (loss) from operations	589,926	142,942	(4,748,494)
Adjusted EBITDA	1,564,245	1,361,548	951,740
Net income (loss) attributable to Yahoo! Inc.	1,366,281	7,521,731	(4,359,082)
Net cash provided by (used in) operating activities	1,195,247	916,350	(2,383,422)
Free cash flow[122]	786,465	586,632	(3,010,172)
Includes:			
Stock-based compensation expense	278,220	420,174	457,153
Restructuring charges, net	3766	103,450	104,019
Asset impairment charge	—	—	44,381
Goodwill impairment charge	63,555	88,414	4,460,837
Intangibles impairment charge	—	—	15,423

Table 2 provides selected consolidated financial operations data and the consolidated balance sheets data for 2011, 2012, 2013, 2014, and 2015.

Table 2: Yahoo Selected Financial Data[123]

Item	Amount (in thousands of dollars, except per share amount) for Years Ended December 31				
	2011	*2012*	*2013*	*2014*	*2015*
Revenue	4,984,199	4,986,566	4,680,380	4,618,133	4,968,301
Total Operating Expenses	4,183,858	4,420,198	4,090,454	4,475,191	9,716,795

121. Yahoo 2015 10-K, *supra* note 104, at 41, item 7.

122. "During the fiscal year that ended December 31, 2015, [Yahoo] satisfied the $3.3 billion income tax liability related to the sale of Alibaba Group American Depositary Shares (ADSs) in Alibaba Group's initial public offering ('Alibaba Group IPO') in September 2014." *Id.*

123. Yahoo 2015 10-K, *supra* note 104, at 37, item 6. Footnotes 3, 4, 5, 6, and 7 have been omitted from this presentation but may be found on page 38 of Form 10-K for the Period Ended Dec. 31, 2015.

Income (Loss) from Operations	800,341	566,368	589,926	142,942	(4,748,494)
Other Income (Expense), Net[1]	27,175	4,647,839	43,357	10,369,439	(75,782)
(Provision) Benefit for Income Taxes	(241,767)	(1,940,043)	(153,392)	(4,038,102)	89,598
Earnings in Equity Interests	476,920	676,438	896,675	1,057,863	383,571
Net Income (Loss) Attributable to Yahoo! Inc.	1,048,827	3,945,479	1,366,281	7,521,731	(4,359,082)
Net Income (Loss) Attributable to Yahoo! Inc. Common Stockholders Per Share—Basic	0.82	3.31	1.30	7.61	(4.64)
Net Income (Loss) Attributable to Yahoo! Inc. Common Stockholders Per Share—Diluted	0.82	3.28	1.26	7.45	(4.64)
Shares Used in Per Share Calculation—Basic	1,274,240	1,192,775	1,052,705	987,819	939,141
Shares Used in Per Share Calculation—Diluted	1,282,282	1,202,906	1,070,811	1,004,108	939,141
Includes:					
Stock-Based Compensation Expense	203,958	224,365	278,220	420,174	457,153
Restructuring Charges, Net	24,420	236,170	3766	103,450	104,019
Includes:					
Gain on Sale of Alibaba Group Shares	—	4,603,322	—	—	—
Gain on Sale of Alibaba Group ADSs	—	—	—	10,319,437	—

As shown in Table 2, when Yahoo's sale of Alibaba stock for $10.369 billion during 2014 is removed, ongoing operating results appear even more severe. When highlighting Consolidated Statements of Operations Data for just Net Income (loss) attributable to Yahoo, note the substantial decline in income from operations during the fiscal year that ended December 31, 2015. The downward trend in results from operations during years 2013, 2014, and 2015 likely resulted in the Board's decision to offer the Company for sale.

With a goal of maximizing shareholder value, for many years the Yahoo board of directors and management examined various alternatives to optimizing the value of its equity positions in both Alibaba and Yahoo Japan. Given the market value of Yahoo's component parts—Yahoo and its net cash position, Alibaba, and Yahoo Japan—the Yahoo board considered Yahoo's stock price to be significantly undervalued and believed

> at that time that separating Yahoo's equity stakes in Alibaba and Yahoo Japan from its core operating business would create value by, among other things: providing the investor community with greater clarity and focus with respect to the value of Yahoo's operating business; enabling the management of Yahoo to focus exclusively on its operating business; enhancing Yahoo's ability to attract, retain, and incentivize management and employees by creating equity-based compensation that more accurately and efficiently reflects the performance of Yahoo's operating business; and enhancing Yahoo's ability to pursue strategic acquisitions by creating a more efficient equity currency.[124]

This complex analysis explored both taxable and tax-efficient scenarios for monetizing these equity interests and involved the expertise of a number of internationally recognized investment banks, accounting firms, and law firms.[125]

As Yahoo's board continued to explore how best to separate its equity position in Alibaba from Yahoo's operating business, it announced plans to spin-off the remaining holdings in Alibaba on January 27, 2015.[126] Approximately nine months later, the IRS informed Yahoo's legal counsel, Skadden, Arps, Slate, Meagher & Flom LLP ("Skadden Arps"), that a favorable tax ruling for the

---

124. *See* Preliminary Proxy Statement, *supra* note 102, at 36.

125. *Id.* at 35–36 (maintaining that these efforts were among the primary events that led to "the execution of the Stock Purchase Agreement").

126. *Id.* at 36 (emphasizing that the transaction was at first contingent on a favorable ruling by the IRS that would allow Yahoo's counsel to opine that the transaction would receive "tax-free treatment").

proposed spin-off would not be forthcoming.[127] As a result, the Yahoo board announced on December 9, 2015, that work on the proposed spin-off had been suspended.[128] Subsequently, the Yahoo board considered the feasibility, timing, and potential tax implications of alternatives, including the sale of Yahoo's operating business.[129]

Yahoo's telephonic board meeting on January 31, 2016, was attended by representatives of investment banks Goldman Sachs and J.P. Morgan, and counsel from law firms Skadden Arps and Wilson Sonsini Goodrich & Rosati ("Wilson Sonsini").[130] At the meeting, the Yahoo board authorized formation of a special committee of independent directors to consider and evaluate possible strategic transactions involving Yahoo's operating businesses.[131] This initial Strategic Review Committee ("SRC") consisted of Maynard G. Webb, serving as Chairman; H. Scott Lee, Jr.; and Thomas J. McInerney.[132] Also at this time, the Yahoo board authorized the SRC to retain, at Yahoo's expense, "such outside counsel, financial advisors, and other outside advisors" as deemed necessary to carry out its prescribed duties.[133] Moreover, Yahoo's board determined that it would not approve "any strategic transaction related to Yahoo's operating business" unless the SRC recommended such a transaction.[134]

Along with its quarterly and year-end 2015 annual financial results on February 2, 2016, Yahoo announced that its board would explore "strategic alternatives for separating Yahoo's operating business from its Alibaba shares," including a reverse spin-off transaction.[135] Subsequently, the Company's financial advisors contacted fifty-one parties to explore their potential interest in a viable transaction,

---

127. *Id.*
128. *Id.* at 37.
129. *Id.*
130. *Id.*
131. *Id.* at 38.
132. *Id.*
133. *Id.* For more information on special committees and independent counsel, see generally Geoffrey C. Hazard, Jr. & Edward B. Rock, *A New Player in the Boardroom: The Emergence of the Independent Directors' Counsel*, 59 Bus. Law. 1389 (2014) (providing an overview on independent counsel and special committees of the board and discussing, generally, how changes in stock exchange regulation has mandated their implementation in many instances). *See* Audra L. Boone & J. Harold Mulherin, How do Corporate Boards Balance Monitoring and Advising? The Situational Use of Special Committees in Corporate Takeovers 40 (Dec. 2013) (unpublished manuscript), https://ssrn.com/abstract=1783064 (suggesting that of 845 sampled takeovers between 2003 and 2007, special committees were implemented 24% of the time).
134. Preliminary Proxy Statement, *supra note* 102, at 38.
135. *Id.*

executing confidentiality agreements with thirty-two of these parties between February 19 and April 6, 2016.[136] Yahoo provided interested parties access to a virtual data room along with management presentations and three years of forecasted financial information previously reviewed by Yahoo's board.[137] Over time, potential investors continued analysis activities, and the Yahoo board and its SRC continued to meet.[138] However, the composition of the SRC changed, with Mr. Scott resigning and Catherine J. Friedman and Eric K. Brandt being appointed as independent Yahoo directors "to fill vacancies."[139]

During the last two weeks of March 2016, Yahoo management conducted half-day presentations to seven potentially interested parties, including Verizon.[140] Also during this period, the Company communicated proper guidelines for non-binding indications of interest with a deadline of April 11, 2016.[141] Fourteen parties indicated interest on April 18, 2016, so the Company and its financial advisors reviewed and compared these first-round proposals.[142] On April 20 and 21, 2016, the SRC held meetings to review first-round proposals and determine which of these bidders it should encourage to participate in the next-round.[143] Yahoo reported that, following these discussions, the SRC concluded the board should pursue selling Yahoo's entire operating business "through a competitive auction process," which could maximize value for Yahoo's stockholders while also noting that alternative deal structures could still be considered later on.[144]

At this point in the bid process, on April 26, 2016, Yahoo reached a proxy fight settlement with activist investors Starboard Value LP and some of their affiliates, which involved Yahoo's 2016 annual meeting election of directors.[145] In the settlement, Yahoo not only agreed to name several new members to its Board and to the SRC but also "to submit to a stockholder vote any decision recommended by the SRC and approved by the board to sell Yahoo's operating business or any similar transactions."[146]

---

136. *Id.* at 39.
137. *Id.*
138. *Id.*
139. *Id.* at 40.
140. *Id.*
141. *Id.*
142. *Id.* at 41.
143. *Id.* at 42.
144. *Id.* at 42–43.
145. *Id.* at 43.
146. *Id.*

Given what we now know about the massive 2014 data breach, May 12, 2016, may undertake particular significance depending on how much the Yahoo Board and senior management knew about the breach.[147] Via the virtual data room, Yahoo disclosed to potential bidders initial drafts of proposed purchase and reorganization agreements.[148] Given its potential importance, Yahoo's disclosure states the following:

> To minimize the liabilities that would be retained by Yahoo post-closing, the initial draft purchase agreement was structured similar to a typical purchase agreement in a public company acquisition, with no post-closing indemnity by Yahoo and limited closing conditions. In addition, the initial draft purchase agreement provided, in the case of a strategic buyer, that Yahoo's unvested employee equity awards would be assumed or substituted for comparable buyer equity awards, and, in the case of a financial sponsor buyer, that these awards would be accelerated at closing. The draft purchase agreement also provided that Yahoo would be required to pay the buyer a termination fee equal to 2.5 percent of the base purchase price if, among other reasons, the purchase agreement was terminated by the purchaser after the Board changed its recommendation for the transaction or by Yahoo to accept a superior proposal (the "Yahoo termination fee"), and, in the case of a financial sponsor buyer, that Yahoo would be entitled to a reverse termination fee equal to 7.5 percent of the base purchase price if the buyer did not consummate the transaction as a result of its debt financing not being available (the "reverse termination fee"), and to specific performance if the buyer's debt financing was available.[149]

Given what we know now about the extent of knowledge within Yahoo about the data breaches, this language appears to be a clear attempt to shift the cost of cyber liability onto an acquiring entity. In any event, Yahoo's attempts to minimize post-closing liabilities has only partially worked as evidenced by Verizon's renegotiated acquisition announcement that includes cyber liability cost sharing between the two companies.

As of May 13, 2016, nine active bidders remained, and Yahoo notified them about the guidelines and process for submitting their interim non-binding proposals for acquisition of Yahoo's operating business no later than June 6, 2016.[150] It also instructed bidders to

147. *See infra* notes 185–87 and accompanying text (relating that some Yahoo employees knew of the breach in real time and that Mayer knew no later than July 2016).

148. *Id.* at 44.

149. *Id.* at 44.

150. *Id.*

submit a list of key issues in their transaction agreement drafts.[151] The remaining bidders conducted considerable due diligence activity during the end of May and the beginning of June, culminating in Yahoo's receipt of six non-binding interim proposals on June 6, 2016.[152] Numerous discussions between the six remaining bidders and Yahoo's financial advisors continued thereafter in efforts to clarify terms and understand any changes in valuations from initial indications of interest.[153] For instance, between June 13 and 19, Yahoo's outside consultants communicated with each of the remaining bidders to respond to any issues the bidders raised in their interim bids.[154] At the same time, the SRC relayed to bidders upcoming deadlines."[155]

At Yahoo's SRC meeting on June 16, 2016, the SRC "expressed a desire for bidders to be guided to submit final mark-ups of the transaction agreements that would enable Yahoo to be in a position to enter into definitive transaction agreements with the winning bidder as soon as possible after final bids were received."[156] Between June 20 and 24, 2016, each of the remaining five bidders submitted proposals in the form of initial markups of the transaction agreements.[157] During the days that followed, Yahoo's attorneys and financial advisors discussed and clarified proposed transaction terms, resulting in five detailed proposals (three with executed financing commitments) being received by Yahoo and reported in detail within the Yahoo proxy material.[158] Following multiple conference calls to discuss these proposals with Yahoo's financial advisors, the SRC recommended that Yahoo should "negotiate definitive transaction agreements with Verizon on an expedited basis," based upon the following:

- Verizon's bid offered the highest base purchase price;
- Verizon had submitted the transaction agreement mark-ups that were most responsive to the Strategic Review Committee's concerns regarding value, certainty of closing, and leaving the post-closing entity with limited liabilities unrelated to the assets retained by Yahoo;

151. *Id.*
152. *Id.* at 45.
153. *Id.* at 46.
154. *Id.* at 47.
155. *Id.*
156. *Id.*
157. *Id.*
158. *Id.* at 47–50.

- Verizon had sufficient funds to finance the transaction, whereas the financing of the financial sponsor bidders was less certain; and
- Verizon had substantially completed its due diligence review, whereas the financial sponsors needed additional time to complete their due diligence review.[159]

During the days immediately following, Yahoo's lawyers and financial advisors continued to negotiate definitive transaction agreements with Verizon on an expedited basis.[160] Revised drafts of the agreement were circulated.[161] On numerous occasions throughout this process, Yahoo's lawyers reviewed with the SRC their fiduciary duties and other relevant legal considerations.[162] Then, at a Yahoo board meeting held on the evening of July 22, 2016, the terms and conditions of the Verizon offer were reviewed, following discussion by attorneys of the Yahoo board's fiduciary duties, the scope of authority delegated to the SRC by the Yahoo board, and certain other matters, including the insufficiency of a proposal received by Yahoo after the decision to move forward with the Verizon offer.[163] Each of Yahoo's financial advisors (J.P. Morgan, PJT Partners, and Goldman Sachs) rendered their fairness opinions, stating that "the Cash Consideration to be paid in the Sale Transaction . . . pursuant to the purchase agreement, was fair, from a financial point of view."[164]

The July 22, 2016 Yahoo board meeting then recessed so that the SRC could meet in an executive session, at which time the SRC unanimously recommended to the full Yahoo board to approve the purchase agreement and all other associated negotiated agreements with Verizon.[165] Following the SRC's recommendation, the Yahoo board reconvened and, by unanimous vote of all directors present,

- determined that the Sale Transaction Agreements and the Sale Transaction [were] expedient and for the best interests of Yahoo and its stockholders,
- approved the Sale Transaction Agreements and the Sale Transaction,

159. *Id.* at 50–51.
160. *Id.* at 51.
161. *Id.*
162. *Id.*
163. *Id.* at 52.
164. *Id.*
165. *Id.*

- recommended, subject to the terms of the Stock Purchase Agreement, that the Yahoo stockholders adopt a resolution authorizing the Sale Transaction, and
- directed that the Sale Transaction be submitted for consideration by the stockholders at the special meeting.[166]

With this unanimous vote, Yahoo's directors and officers sought shareholder approval of the Verizon acquisition detailed below.

B. The Verizon Acquisition

On July 23, 2016, the parties entered into a Stock Purchase Agreement, providing that Verizon purchase all of Yahoo's outstanding shares of Yahoo Holdings for a cash purchase price of $4,825,800,000, subject to certain adjustments as provided for within the contract for sale.[167]

As renegotiations stemming from the data breach disclosures continued in early 2017, Yahoo announced on January 10, 2017, that when the Company completes the Verizon deal, Yahoo will "whittle down its board" by six members, with several longtime directors—including CEO Marissa Mayer and co-founder David Filo—stepping down from the board.[168] Upon sale of its core internet business to Verizon, the remaining entity will rename itself Altaba, Inc., and Altaba's remaining assets will include Yahoo's stake in Alibaba Group Holdings Ltd. and Yahoo Japan.[169]

On February 15, 2017, news of a renegotiated deal between Verizon and Yahoo leaked, and the leak asserted that the two companies had agreed on a new price $250 million lower than their initial agreement.[170] But on February 21, 2017, when Verizon disclosed the renegotiated deal to acquire Yahoo's core Internet business, Verizon announced a $350 million discount.[171] The renegotiated price brings the original $4.8 billion price down to

---

166. *Id.*

167. *Id.* at 52–53.

168. Deepa Seetharaman & Maria Armental, *Marissa Mayer to Leave Yahoo Board; Yahoo to Change Name to Altaba*, WALL ST. J. (Jan. 10, 2017), http://www.wsj.com/articles/after-sale-marissa-mayer-to-leave-yahoo-board-yahoo-to-change-name-to-altaba-1484002787.

169. *Id.*

170. Scott Moritz, Alex Sherman & Brian Womack, *Verizon Said to Near Yahoo Deal at Lower Price After Hacks*, BLOOMBERG (Feb. 15, 2017, 2:47 PM), https://www.bloomberg.com/news/articles/2017-02-15/verizon-said-to-reach-revised-price-for-yahoo-in-wake-of-hacks.

171. Seth Fiegerman, *Verizon Cuts Yahoo Deal Price by $350 Million*, CNN (Feb. 21, 2017, 9:12 AM), http://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal.

$4.48 billion.[172] Further, "Verizon and the entity that remains of Yahoo after the deal, . . . Altaba Inc., are expected to share any ongoing legal responsibilities related to the breaches."[173] The deal closed on June 8, 2017.[174]

Table 3 depicts selected financial data for Verizon for the periods ending December 31, 2015, for the years indicated.

Table 3: Verizon Communications, Inc. Selected Financial Data[175]

Results of Operations	Amount (in millions of dollars, except per share amount) for Years Ended December 31				
	2011[176]	*2012*[177]	*2013*	*2014*	*2015*
Operating Revenues	110,875	115,846	120,550	127,079	131,620
Operating Income	12,880	13,160	31,968	19,599	33,060
Net Income Attributable to Verizon	2,404	875	11,497	9,625	17,879
Per Common Share—Basic	0.850	0.310	4.010	2.420	4.380
Per Common Share—Diluted	0.850	0.310	4.000	2.420	4.370
Cash Dividends Declared Per Common Share	1.975	2.030	2.090	2.160	2.230
Net Income Attributable to Noncontrolling Interests	7,794	9,682	12,050	2,331	496
Financial Position					
Total Assets	228,194	222,911	273,654	232,616	244,640
Debt Maturing Within One Year	4,849	4,369	3,933	2,735	6,489
Long-Term Debt	50,303	47,618	89,658	110,536	103,705
Employee Benefit Obligations	32,957	34,346	27,682	33,280	29,957
Noncontrolling Interests	49,938	52,376	56,580	1,378	1,414

172. *Id.*

173. Moritz, Sherman & Womack, *supra* note 170.

174. Deepa Seetharaman, *Yahoo's Marissa Mayer to Make $186 Million from Verizon Deal*, FOX BUS. (Apr. 25, 2017), http://www.foxbusiness.com/markets/2017/04/25/yahoos-marissa-mayer-to-make-186-million-from-verizon-deal.html.

175. VERIZON, 2015 ANNUAL REPORT, *supra* note 6, at 9.

176. "2011 data includes severance, pension and benefit charges and early debt redemption costs." *Id.*

177. "2012 data includes severance, pension and benefit charges, early debt redemption costs and litigation settlement charges." *Id.*

Equity Attributable to Verizon	35,970	33,157	38,836	12,298	16,428

C. The Breaches

On September 22, 2016, Yahoo announced (what was at that time) "the largest data breach in history—affecting at least 500 million user accounts."[178] Yahoo's statement on the breach disclosed that user information—which included names, email addresses, telephone numbers, birth dates, encrypted passwords and, in some cases, security questions—was compromised in late 2014.[179] Further, Yahoo's statement alleged that an unnamed "state-sponsored actor" was responsible for the breach.[180] In March 2017, the U.S. Department of Justice indicted two Russian intelligence officers for "directing a sweeping criminal conspiracy" to hack Yahoo in 2014 and steal more than 500 million Yahoo users' personal information.[181]

Then, on December 14, 2016, Yahoo disclosed an earlier and even larger data breach than the 2014 breach disclosed in September 2016.[182] This attack occurred in 2013 and exposed more than one billion accounts, which "involved sensitive user information, including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password."[183] It is, however, unclear how many of the same user accounts were compromised in the 2013 and 2014 data breaches; Yahoo has more than one billion active users, but there is lingering uncertainty about the number of inactive accounts that were hacked.[184]

Table 4 depicts the top ten breaches of all time and is helpful in placing the Yahoo breaches—the two largest ever—into perspective with other major data breaches.

---

178. Hayley Tsukayama, Craig Timberg & Brian Fung, *Yahoo Data Breach Casts "Cloud" over Verizon Deal*, WASH. POST: THE SWITCH (Sept. 22, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts.

179. *Yahoo Press Release*, *supra* note 1.

180. *Id.*

181. Vindu Goel & Eric Lichtblau, *Russian Agents Were Behind Yahoo Hack, U.S. Says*, N.Y. TIMES (Mar. 15, 2017), https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html.

182. Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

183. *Id.*

184. *Id.*

Table 4: Top 10 Data Breaches of All Time as of 2016[185]

Rank: Date Reported	*Summary*	*Records Exposed*	*Org. Name*	*Industry, Sector*	*Breach Location*
New Record? 12/14/2016	Hack exposed names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions and answers.	1 Billion	Yahoo	Business, Technology	United States
#1: 9/22/2016	Hack exposed user names, email addresses, phone numbers, dates of birth, hashed passwords, and security questions and associated answers.	500 Million	Yahoo	Business, Technology	United States
#2: 5/27/2016	Hack exposed user account records containing email addresses and SHA1 encrypted passwords.	360 Million	MySpace	Business	United States
#3: 8/22/2014	Hack of websites exposed names, registration numbers, usernames, and passwords.	220 Million	Not Reported	Unknown	South Korea
#4: 10/19/2013	Fraudulent account created gaining access to credit card numbers, social security numbers, names, and financial account numbers.	200 Million	Court Ventures, Inc.	Business, Data	United States
#5: 12/28/2015	Mis-configured database exposes voter names, dates of birth, addresses, phone numbers, political party affiliations, and genders.	191 Million	Not Reported	Unknown	United States
#6: 6/21/2014	Hack exposed trip details of customers after de-anonymizing MD5 hashes.	173 Million	NYC Taxi & Limousine	Government, City	United States
#7: 6/23/2016	Hack exposed USA voter information.	154 Million	Not Reported	Unknown	United States

185. DATA BREACH QUICKVIEW REPORT: 2016 DATA BREACH TRENDS—YEAR IN REVIEW 14 (2016), https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf (listing *exposed* hacks).

#8: 10/3/2013	Hack exposed customer names, IDs, encrypted passwords, and debit/credit card numbers with expiration dates, source code and other customer order information.	152 Million	Adobe Systems, Inc.	Business, Technology	United States
#9: 3/17/2012	Firm may have illegally bought and sold customers' information.	150 Million	Shanghai Roadway D&B	Business, Data	China
#10: 5/21/2014	Hack exposed names, encrypted passwords, email addresses, registered addresses, phone numbers, and dates of birth.	145 Million	eBay, Inc.	Business, Retail	United States

Notwithstanding the magnitude of the security breaches, considerable controversy surrounds the timing of when Yahoo employees learned of the 2014 breach. Despite representing in a September 9, 2016 SEC filing that Yahoo was not aware of any security breaches[186]—and a recent disclosure that at least some Yahoo employees were aware of the breach in 2014[187]—most current accounts of internal knowledge of the breach maintain that CEO Marissa Mayer was aware of it in late July 2016.[188]

Because of the security breaches, many questions arise regarding the corporate duties of Yahoo executives. The discussion below first

186. *See* Preliminary Proxy Statement, *supra* note 102, Exhibit A-18 ("To the Knowledge of [Yahoo], there have not been any incidents of, or third party claims alleging, (i) Security Breaches, unauthorized access or unauthorized use of any of [Yahoo's]... information technology systems or (ii) loss, theft, unauthorized access or acquisition, modification, disclosure, corruption, or other misuse of any Personal Data in [Yahoo's] possession... that could reasonably be expected to have a Business Material Adverse Effect.").

187. *See* Yahoo! Inc., SEC Quarterly Report (Form 10-Q), at 40 (Nov. 9, 2016), http://files.shareholder.com/downloads/YHOO/4041065081x0xS1193125-16-764376/1011006/filing.pdf (disclosing that "[Yahoo] had identified that a state-sponsored actor had access to the Company's network in late 2014"); *see also* Vindu Goel, *Yahoo Employees Knew in 2014 About State-Sponsored Hacker Attack*, N.Y. TIMES (Nov. 9, 2016), http://www.nytimes.com/2016/11/10/technology/yahoo-employees-knew-in-2014-about-hacker-attack.html.

188. *See* Madhumita Murgia, Tim Bradshaw & David J. Lynch, *Marissa Mayer Knew of Yahoo Breach Probe in July*, FIN. TIMES (Sept. 23, 2016), https://www.ft.com/content/d0d07444-81aa-11e6-bc52-0c7211ef3198.

details facts relevant to whether Yahoo executives breached their duty to provide security with a specific emphasis on Yahoo's cybersecurity and data privacy practices before senior management definitively learned of the breach in July 2016; second are facts relevant to whether Yahoo executives breached their duty to monitor and be informed; third and finally are facts relevant to whether Yahoo executives breached their duty to disclose the existence of the breach sooner than they did.

1. Facts relevant to Yahoo's duty to provide security

In 2010, Chinese military hackers breached several major Silicon Valley technology corporations, including Google, Inc., and Yahoo.[189] Google responded by designating cybersecurity "a top corporate priority"[190]: the company hired hundreds of handsomely-compensated cybersecurity engineers, invested hundreds of millions of dollars in securing the fidelity of its data infrastructure, and "adopted a new internal motto, 'Never again,' to signal that it would never again allow anyone . . . to hack into Google customers' accounts."[191] In contrast, Yahoo's response was considerably slower and less robust, according to at least six current and former Yahoo employees who were involved in cybersecurity discussions and decision making and who related these internal deliberations to the *New York Times* in the wake of Yahoo's disclosure of the 2014 data breach.[192]

Although Yahoo's former CEO Marissa Mayer was recruited in 2012—from security-conscious Google—to stage a turnaround for the flagging corporation, amid a slew of competing priorities, Ms. Mayer reportedly did not emphasize cybersecurity.[193] In fact, in stark contrast to Google's "Never Again" motto, Yahoo's cybersecurity team was internally dubbed the "Paranoids," and they often clashed with other aspects of the Company—particularly over the cost of enhancing Yahoo's IT security.[194] In addition to cost concerns, Yahoo often impeded the cybersecurity team's ability to effectively carry out its mission out of a pervasive fear that "the inconvenience of added

189. Nicole Perlroth & Vindu Goel, *Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say*, N.Y. TIMES (Sept. 28, 2016), http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html.

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.* (explaining that Ms. Mayer denied Yahoo's security team support and funds needed to take proactive security measures, like implementing intrusion-detection mechanisms for the company's production systems).

protection would make people stop using the company's products."[195] These dual cost-related concerns—the direct, tangible dollar cost of implementing more thorough cybersecurity practices and the indirect (though potentially more severe) cost of losing customers—help explain many shortcomings of Yahoo's cybersecurity practices.

Four specific examples of Yahoo's seemingly lax commitment to corporate cybersecurity from the *New York Times* report illustrate the shortcomings of Yahoo's security. First, Yahoo did not begin compensating hackers for providing the Company with information on digital vulnerabilities until 2013—three years after Google adopted the same policy—and Yahoo adopted the policy only "after it lost countless security engineers to competitors and experienced a breach of more than 450,000 Yahoo accounts in 2012 and a series of humiliating spam attacks in 2013."[196]

Second, even after it took Yahoo a year to hire a new chief information security officer ("CISO") following former U.S. National Security Agency contractor Edward Snowden's disclosure of damaging information—which revealed that Yahoo was a constant target for nation-state spies—Yahoo failed to empower, and denied requested resources to, its new CISO.[197]

Outsiders initially hailed the 2014 hiring of CISO Alex Stamos, who left the Company in 2015, as potentially signaling a renewed corporate commitment to cybersecurity.[198] But Mr. Stamos frequently clashed with Mayer and Yahoo's senior vice president, Jeff Bonforte, who oversaw Yahoo's email and messaging services.[199] For example, Mr. Bonforte revealed in a December 2015 interview that Mr. Stamos had quickly pressed senior management to adopt end-to-end encryption for the Company's entire digital infrastructure, which would prevent Yahoo from being able to read the content of users' communications.[200] Mr. Bonforte resisted the recommendation because doing so would hinder the Company's ability to index and search message data, precluding it from tailoring new, additional user services.[201]

---

195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.* Mr. Bonforte expressly confirmed his resistance to Mr. Stamos's end-to-end encryption recommendation, stating, "I'm not particularly thrilled with building an apartment building which has the biggest bars on every window." *Id.*

Third, Ms. Mayer repeatedly refused to invest meaningful resources to secure Yahoo's security infrastructure—to the chagrin of Mr. Stamos and his team. According to the half-dozen insiders, Ms. Mayer "denied Yahoo's security team financial resources and put off proactive security defenses, including intrusion-detection mechanisms for Yahoo's production systems."[202] Some commentators have deemed Ms. Mayer's refusal to invest in Mr. Stamos's team and follow their recommendations a major contributor to a mass exodus from the Company's cybersecurity team that Mr. Stamos assembled.[203] According to the publication *Recode*, "[o]ne executive close to the situation said that former Yahoo information security head Alex Stamos had tried aggressively to get management to act more strongly at the time, but he had not been successful," which ultimately led to Mr. Stamos' resignation from Yahoo and move to Facebook as chief security officer in mid-2015.[204]

Fourth and finally, Ms. Mayer rejected the suggested implementation of one of the most basic security measures: automatically resetting all users' passwords, "a step security experts consider standard after a breach."[205] Ms. Mayer's rationale for rejecting such a fundamental staple of data breach response derived from a "fear that even something as simple as a password change would drive Yahoo's shrinking email users to other services."[206] Indeed, a Yahoo spokesperson confirmed this continues to be the Company's policy: "Yahoo's policy is that if we believe a user's password has been compromised, we lock the account until the user resets the password."[207]

For its part, Yahoo has pushed back against the narrative that its cybersecurity practices prior to discovery and disclosure of the 2014 data breach were inadequate. For instance, a Company spokesperson told the *New York Times* that "the company spent $10 million on encryption technology in early 2014, and that its investment in security initiatives will have increased by 60 percent from 2015 to

---

202. *Id.*

203. *Id.* (stating that many Paranoids left Yahoo for competitors like Apple, Facebook, and Google in recent years).

204. Kara Swisher & Kurt Wagner, *Yahoo Has Confirmed a Data Breach with 500 Million Accounts Stolen, as Questions About Disclosure to Verizon and Users Grow*, RECODE (Sept. 22, 2016), http://www.recode.net/2016/9/22/13021300/yahoo-hack-data-breach-500-million-accounts-stolen.

205. Perlroth & Goel, *supra* note 189.

206. *Id.*

207. *Id.*

2016."[208] Nonetheless, the recently disclosed 2013 breach, which compromised more than one billion user accounts, further undermines Yahoo's claim that its data security practices were adequate.[209] Jay Kaplan, the chief executive of the data security company Synack, made a succinct case to the *New York Times* for how these most recent disclosures support the narrative that Yahoo's data security practices were grossly deficient over a period of years: "What's most troubling is that this occurred so long ago, in August 2013, and no one saw any indication of a breach occurring until law enforcement came forward."[210]

On March 1, 2017, Yahoo announced the results of an internal investigation into the Company's handling of the data breaches.[211] Ronald Bell, Yahoo's General Counsel, resigned, and Mayer's pay would be docked about $14 million dollars—the result of giving up a 2016 cash bonus and foregoing a 2017 stock award.[212] The blame lay with Bell because, according to the Company, "the Committee found that the relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it."[213]

2. Facts relevant to Yahoo's duty to monitor

We now turn to address facts concerning the adequacy of Yahoo's internal monitoring and reporting processes. The facts related in this section are later implicated in our analysis of whether Yahoo's monitoring and reporting procedures fell below the standard of care necessitated by the duty to monitor.

Yahoo recently disclosed that at least some Yahoo employees knew of the 2014 data breach in nearly real-time.[214] This revelation raises questions about the adequacy of Yahoo's internal monitoring and reporting processes. In a September 30, 2016 filing with the SEC, Yahoo "identified that a state-sponsored actor had access to the

208. *Id.*
209. *Id.*
210. *Id.*
211. Kara Swisher, *Yahoo's Head Lawyer Is Taking the Fall for Its Hacking, While CEO Marissa Mayer Is Getting Her Pay Docked*, RECODE (Mar. 1, 2017, 5:33 PM), https://www.recode.net/2017/3/1/14783686/yahoos-lawyer-ousted-hacking-marissa-mayer-pay-docked.
212. *Id.*
213. Yahoo 2015 10-K, *supra* note 104, at 47.
214. Hannah Kuchler, *Yahoo Admits Some Staff Knew of Hacking in 2014*, FIN. TIMES (Nov. 9, 2016), https://www.ft.com/content/ce7a4784-a6ca-11e6-8b69-02899e8bd9d1.

Company's network in late 2014."[215] The filing further disclosed that an independent committee of Yahoo's board of directors had launched an investigation into the "scope of the knowledge within the Company in 2014."[216] Additionally, the filing suggested, troublingly, that a hacker may have created the means to forge Yahoo Mail cookies to allow access without requiring a password.[217] This disclosure raises the specter that a hacker could continue to have unfettered access to Yahoo Mail users' accounts even after users reset their passwords.[218] However, a person close to Yahoo's internal investigation "said Yahoo did not believe it was currently possible for attackers to forge the Yahoo Mail cookies."[219]

The recently disclosed 2013 breach that compromised more than one billion user accounts contradicts Yahoo's claim that its monitoring and reporting systems were adequate. In fact, Yahoo itself did not even discover the 2013 data breach: according to media reports, Yahoo "discovered the larger hacking after analyzing data files, provided by law enforcement, that an unnamed third party had claimed contained Yahoo information."[220]

On March 1, 2017, Yahoo filed its Annual Report with the SEC and in it the Company made several new disclosures about the extent of internal knowledge of the breaches and the failure of its reporting and monitoring systems.[221] According to Yahoo, the investigation found that "the Company's information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016," and that "[i]n late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool."[222]

---

215. Yahoo! Inc., Quarterly Report (Form 10-Q) (Nov. 9, 2016) [hereinafter Yahoo Nov. 10-Q], https://www.sec.gov/Archives/edgar/data/1011006/000119312516764376/d244526d10q.htm.

216. *Id.* *Compare* Swisher & Wagner, *supra* note 204 (reporting that Mayer knew about the security breach in early August 2016), *with* Murgia, Bradshaw & Lynch, *supra* note 186 (reporting that Mayer knew about the security breach in late July 2016).

217. Yahoo Nov. 10-Q, *supra* note 215.

218. Kuchler, *supra* note 214.

219. *Id.*

220. *See* Goel & Perlroth, *supra* note 182.

221. *See* Yahoo! Inc., Annual Report (Form 10-K) (Mar. 1, 2017) [hereinafter Yahoo 2016 10-K], https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm.

222. *Id.* at 47.

The report details management's efforts to respond to these threats but notes that "it appears certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team."[223] Specifically, according to Yahoo, "as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users but it is unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team."[224] This finding, put simply, means that Yahoo's internal digital security team knew in December 2014 that a hacker had successfully copied large portions of the Company's database—which included the personal data of hundreds of millions of Yahoo users—but it is "unclear whether and to what extent" that knowledge was communicated to senior management.

Despite this explicit lack of clarity regarding "whether and to what extent" senior management knew what the information security team knew in December 2014, the report boldly claims that "the Independent Committee did not conclude that there was an intentional suppression of relevant information."[225] And yet, according to Yahoo, "the Committee found that the relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it," and, as a result of that failure, "the 2014 Security Incident was not properly investigated and analyzed at the time, and the Company was not adequately advised with respect to the legal and business risks associated with the 2014 Security Incident."[226]

The report concludes, "The Independent Committee found that failures in *communication, management, inquiry and internal reporting* contributed to the lack of proper comprehension and handling of the 2014 Security Incident."[227]

3. Facts relevant to Yahoo's duty to disclose

Concern over the conduct of Yahoo's senior management is not limited to what senior management did and did not do prior to learning about the 2014 data breach in July 2016. Management's

223. *Id.*
224. *Id.*
225. *Id.*
226. *Id.*
227. *Id.* (emphasis added).

failure to notify its shareholders, its potential acquirers, and regulators—appearing to have publicly misrepresented the very existence of the 2014 breach—between July 2016 and public disclosure of the breach on September 22, 2016, implicate the duty to disclose.

Although an internal Yahoo investigation found no evidence of a breach, an infamous cybercriminal and hacker, known by the moniker "Peace," revealed the breach on the "dark web" in July or August 2016.[228] The hacker alleged that more than 200 million Yahoo user accounts had previously been compromised and were for sale.[229] Concerns over this allegation, however, allegedly spurred the Company to investigate the claim more deeply; this more sophisticated probe revealed the 2014 breach that affected more than half a billion users' accounts.[230]

Yahoo's senior management has allegedly been involved in investigating the truth of Peace's claims from the beginning. According to a person familiar with Yahoo deliberations on Peace's claims and the 2014 hack,

> Marissa [Mayer] was aware absolutely—she was aware and involved when Peace surfaced this allegation in July . . . [She] was part of the investigation and conversation from the very beginning and along with the team every step of the evidentiary gathering and analysis process. In fact, the key executive team has been engaged from the very beginning.[231]

Despite Ms. Mayer's involvement, internal Yahoo sources bluntly told *Recode* that "the company had been subjected to a number of previous incidents that were not managed swiftly by CEO Marissa Mayer."[232]

Even more, Yahoo failed to disclose the 2014 data breach to three constituencies until approximately two months after senior management learned of the breach. First, the company did not *publicly* disclose—either to its users or to its shareholders—the breach until September 22, 2016.[233] Second, Yahoo did not disclose the breach to potential acquirer Verizon until September 19, 2016—despite Verizon's commitment to acquire Yahoo's core business for $4.8 billion on July 25, 2016.[234] Finally, Yahoo not only failed to

228. *See* Murgia, Bradshaw & Lynch, *supra* note 186; Swisher & Wagner, *supra* note 204.
229. Swisher & Wagner, *supra* note 204.
230. Murgia, Bradshaw & Lynch, *supra* note 186.
231. *Id.*
232. Swisher & Wagner, *supra* note 204.
233. *Id.*
234. Murgia, Bradshaw & Lynch, *supra* note 186; *see also* Paul Szoldra, *In September, Yahoo Told Verizon It Hadn't Been Hacked—But Executives May Have Known for Months,*

disclose the breach to regulators, but it also represented that it was unaware that any breach had occurred. Yahoo filed a document with the SEC on September 9, 2016, with the following representation:

> To the Knowledge of Seller, *there have not been any incidents of, or third party claims alleging,* (i) *Security Breaches,* unauthorized access or unauthorized use of any of Seller's or the Business Subsidiaries' information technology systems or (ii) *loss, theft, unauthorized access or acquisition, modification, disclosure, corruption, or other misuse of any Personal Data in Seller's or the Business Subsidiaries' possession,* or other confidential data owned by Seller or the Business Subsidiaries (or provided to Seller or the Business Subsidiaries by their customers) in Seller's or the Business Subsidiaries' possession, in each case (i) and (ii) that could reasonably be expected to have a Business Material Adverse Effect.[235]

Both Ms. Mayer and Ronald Bell, Yahoo's General Counsel, signed the September 9 SEC filing.[236]

On January 22, 2017, the *Wall Street Journal,* among other sources, announced that the SEC opened an investigation into the timing of Yahoo's disclosure of the breach. Specifically, the SEC sought to uncover whether Yahoo's "two massive data breaches should have been reported sooner to investors."[237] Further, "[l]egal experts say the SEC has been looking for a case to clarify what type of conduct would run afoul of guidance the agency issued in 2011."[238] Unlike previous cases, including the Target Corp. breach in 2013 that compromised as many as 70 million credit cards, the SEC seems to be more confident about bringing its first-breach disclosure enforcement action.[239]

The findings of Yahoo's 2016 Annual Report largely exculpate senior management for its failure to disclose the existence of the breaches much earlier.[240] The report found that "[i]n late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the

---

BUS. INSIDER (Sept. 23, 2016, 7:06 PM), http://www.businessinsider.com/yahoo-deny-security-breaches-2016-9.

235. *See* Preliminary Proxy Statement, *supra* note 102, Exhibit A-18 (emphasis added).

236. *Id.* Exhibits A-73, B-28.

237. Aruna Viswanatha & Robert McMillan, *Yahoo Faces SEC Probe over Data Breaches,* WALL ST. J. (Jan. 23, 2017, 9:56 AM), http://www.wsj.com/articles/yahoo-faces-sec-probe-over-data-breaches-1485133124.

238. *Id.*; *see supra* Section I.C.

239. *See* Viswanatha & McMillan, *supra* note 237 (quoting former SEC lawyers that the Yahoo breach disclosure case "appears to provide a clearer set of circumstances" than previous large breaches).

240. *See* Yahoo 2016 10-K, *supra* note 221, at 47.

Company's account management tool," but that "certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team."[241] This failure to properly comprehend and investigate the Company's security issues in December 2014 is presumably senior management's rationale for its failure to disclose.

The report does not, however, explain why Mayer and Bell made the September 9 misrepresentation to the SEC. But as noted above, Bell has resigned from the Company.[242]

D. Compensation, Code of Ethics, and the Duty to Disclose Material Events

In addition to corporate officers' fiduciary duties, companies also protect their shareholders by generating and relying upon internal mechanisms. Such mechanisms function to deter and remediate issues as they arise. Among the key internal controls, companies rely on (1) executive compensation packages, (2) provisions for "clawbacks" of compensation, (3) severance and change in control provisions, (4) internal ethics policies, and (5) published core values.

Executive compensation has the power to influence corporate decision making, especially amidst a material corporate event. The following table presents compensation information for Yahoo's Named Executive Officers for the years 2013, 2014, and 2015.

241. *Id.*

242. *See id.* ("In response to the Independent Committee's findings related to the 2014 Security Incident, . . . Ronald S. Bell resigned as the Company's General Counsel and Secretary and from all other positions with the Company.").

Table 5: Yahoo Summary Compensation Table[243]

Name and Principal Position	*Year*	Amount (in dollars)						
		Salary	*Bonus*	*Stock Awards*	*Option Awards*	*Non-Equity Incentive Plan Compensation*	*All Other Compensation*	*Total*
Marissa A. Mayer, CEO	2015	1M	1.1k	14.5M	19.9M	-	550k	36M
	2014	1M	-	11.7M	28.2M	1.1M	28k	42M
	2013	1M	2.2k	8.3M	13.8M	1.7M	73.8k	25M
Ken Goldman, CFO	2015	600k	-	3.3M	11M	-	4.6k	15M
	2014	600k	-	2.8M	9.3M	300k	4.5k	13M
	2013	600k	-	2.6M	2.3M	500k	4.6k	6M
David Filo, Co-Founder & Chief Yahoo	2015	1	-	-	-	-	-	1
	2014	1	-	-	-	-	-	1
	2013	1	-	-	-	-	-	1
Lisa Utzschneider, CRO	2015	600k	1M	8.4M	-	-	4.6k	10M
Ronald S. Bell, GC	2015	600k	-	3.9M	-	-	4.6k	4.5M
	2014	600k	-	3.3M	-	300k	4.5k	4.2M
	2013	600k	-	3.9M	-	450k	4.6k	4.9M

As shareholder approval of the Verizon acquisition neared, Yahoo made additional disclosures about the extent of executive compensation. For example, the *New York Times* reported on April 24, 2017, that—based on Yahoo's then-current share price of $48.15, which has since risen—Mayer's payout for the Verizon deal would be more than $186 million.[244] This $186 million is in addition to Mayer's compensation (salary, bonus, and benefits) over the past five years,

243. *See* Yahoo! Inc., Annual Report (Form 10-K/A), Amendment No. 1, 42 (Apr. 29, 2016) [hereinafter Yahoo 2015 10-K/A], https://www.sec.gov/Archives/edgar/data/1011006/000119312516569864/d177362d10ka.htm. Due to space limitations, footnotes appearing in the original document have been either truncated or omitted.

244. Vindu Goel, *Marissa Mayer Will Make $186 Million on Yahoo's Sale to Verizon*, N.Y. TIMES (Apr. 24, 2017), https://www.nytimes.com/2017/04/24/technology/marissa-mayer-will-make-186-million-on-yahoos-sale-to-verizon.html.

which is reportedly in excess of $200 million.[245] As Yahoo's share price has continued to rise, Mayer's all-in compensation for her largely failed tenure leading Yahoo will be approximately $400 million.

In addition to compensation, provisions for "clawbacks" of compensation and severance packages also serve as an internal check that may potentially influence corporate decision making. Yahoo disclosed the following policy regarding its compensation clawback applicable under certain circumstances:

> We maintain a recoupment ("clawback") policy for incentive awards paid to executive officers (including all of the Named Executive Officers). In the event of a restatement of incorrect Yahoo financial results, this policy permits the Board, if it determines appropriate in the circumstances and subject to applicable laws, to seek recovery of the incremental portion of the incentive awards paid or awarded, whether in cash or equity, to our executive officers in excess of the awards that would have been paid or awarded based on the restated financial results.[246]

While Yahoo has entered into change-in-control severance plans with all eligible full-time employees, these arrangements contemplate potential payments in the event that Yahoo terminates certain key employees or in the event that management changes, such as in the case of acquisition by Verizon.[247] While more complex and detailed than depicted here, the following list highlights some of the severance benefits for Ms. Mayer, Mr. Goldman, Ms. Utzschneider, and Mr. Bell:

- one year of base salary;
- one year's target annual bonus;
- if the termination occurs after the end of a fiscal year and before the Company's bonus payments for that fiscal year, the executive's bonus for the completed fiscal year; and
- payments equal to the premiums required to continue medical benefits under COBRA for up to twelve months after termination.

---

245. *Id.*; *see also* Michael Nunez, *Marissa Mayer Set to Receive $186 Million for Failing Because This Is How Corporate America Works*, GIZMODO (Apr. 25, 2017, 11:16 AM), http://gizmodo.com/marissa-mayer-set-to-receive-186-million-for-failing-b-1794625573 ("The [$186 million] sum does not include Mayer's salary or bonuses over the past five years, which reportedly add up to more than $200 million alone.").

246. *See* Yahoo! Inc., Report Filed on Form 10-K/A for the Fiscal Year Ended December 31, 2015, Amendment No. 1, 42 (Apr. 29, 2016) [hereinafter Yahoo 2015 10-K/A], https://www.sec.gov/Archives/edgar/data/1011006/000119312516569864/d177362d10ka.htm.

247. *See id.* at 38.

- The executive will also have six months to exercise any vested Company stock options.[248]

Table 6 presents Yahoo's estimated severance benefits to which each of the following named executive officers would have been entitled as of December 31, 2015, if Yahoo had terminated their employment without cause.

Table 6: Hypothetical Change-in-Control Severance Benefits[249]

Name	Amount (in dollars)					
	Cash Severance	*Continuation of Health Benefits*	*Outplacement Benefits*	*RSU Acceleration*	*Option Acceleration*	*Total*
Marissa A. Mayer	3.0M	26.3k	15k	29.9M	21.9M	54.9M
Ken Goldman	1.2M	54.2k	15k	8.8M	6.0M	16.1M
David Filo	2	54.2k	15k	-	-	69.0k
Lisa Utzschneider	1.2M	54.2k	15k	18.6M	-	19.9M
Ronald S. Bell	1.2M	54.2k	15k	7.8M	-	9.0M

Lastly, a company's internal code of ethics and published core values steer decision making in order to comply with such internal controls. The key policies, fundamental principles, and procedures governing Yahoo's business conduct is set forth in the Company's code of ethics. The Company's contractors, as well as all of its employees and directors, are subject to the code.[250] Within the forty-eight page code of ethics document, "A Message from Yahoo's Board of Directors" strongly emphasizes Yahoo's legacy of integrity and commitment to continue upholding the highest ethical standards.[251]

When discussing the core value of excellence, Yahoo declares "[it is] committed to winning with integrity . . . [and] [it] aspires to flawless execution and [without] tak[ing] shortcuts on quality."[252] Under the category of customer fixation, Yahoo states the following: "[w]e respect

248. *Id.* at 56.
249. *Id.* at 60.
250. *Id.* at 9.
251. *See* YAHOO!, INC., YAHOO'S CODE OF ETHICS: WINNING WITH INTEGRITY 48 (2011), http://files.shareholder.com/downloads/YHOO/660619262x0x239565/4f32ddd0-82e5-47c2-ac71-75403ebbb404/YahooCodeOfEthics_Ext_1008.pdf.
252. *Id.* at 4.

our customers above all else and never forget that they come to us by choice" and "[w]e share a personal responsibility to maintain our customers' loyalty and trust."[253] Lastly, with respect to community, Yahoo "share[s] an infectious sense of mission to make an impact on society and empower consumers in ways never before possible."[254]

Yahoo appears to have all the appropriate boilerplate when it comes to Code of Ethics discussion regarding "[a]ccurate [b]usiness [c]ommunication, [r]ecords, and [c]ontracts."[255] Accordingly, Yahoo states,

> Accurate and reliable business records are critical to meeting our financial, legal, and business obligations. If you are responsible for creating and maintaining Yahoo's financial records, you must do so in accordance with applicable legal requirements and generally accepted accounting practices. Disclosures in reports and documents filed with or submitted to the U.S. Securities and Exchange Commission and other public communications made by Yahoo must be full, fair, accurate, timely, and understandable.[256]

Yahoo's Code of Ethics requires the Company to disclose "clear, truthful, and accurate" information about itself.[257] Furthermore, the Code encourages the public to contact the ECO or Legal Department if one discovers "any omission, inaccuracy, or falsification in Yahoo's business records (or its supporting information)."[258]

Of particular relevance to the 2014 data breach and subsequent disclosure, Yahoo states that, "[c]onflicts of interest can arise in many ways, including . . . [u]sing your position or assignment at Yahoo for personal gain . . . And remember, you may not use other people to do indirectly what you are prohibited from doing yourself."[259]

Regarding data security, Yahoo's Code of Ethics states,

> By protecting our knowledge base and our information systems, we protect our competitive advantage. If you are employed by Yahoo or providing services to Yahoo, you may have access to confidential and/or proprietary information regarding our business, users, advertisers, content providers, vendors, partners, candidates for employment . . . . Protecting this information is vital to our

253. *Id.*
254. *Id.*
255. *Id.* at 13.
256. *Id.*
257. *Id.*
258. *Id.*
259. *Id.*

> success. We are also committed to respecting the intellectual property and protected information of others.[260]

While these declarations are typical and arguably boilerplate, the debacle at Yahoo starkly demonstrates just how hollow corporate commitments can be. Accordingly, the undeniable tension between Yahoo's conduct and its commitments gives rise to the question: Is there a substantial difference between what Yahoo says and what Yahoo does?

E. Timeline of Events

The following Table provides a brief summary of events in chronological order.

Table 7: Timeline Summary of Relevant Events

Year	*Date*	*Event*
2012	July	Marissa Mayer is named CEO of Yahoo.
2013	Sometime in 2013	Yahoo suffers a breach that compromises over 1 billion user accounts, including names, telephone numbers, birthdates, passwords, and security questions.
	June	Snowden disclosures begin. Yahoo is revealed to be a constant target for state-sponsored cyberattacks.
2014	March	Alex Stamos named Chief Information Security Officer.
	Sometime in late 2014	A second Yahoo data breach occurs, which compromises at least 500 million user accounts' sensitive information. At least some Yahoo employees are aware of it.
	November	Sony hack occurs.
2015	June	Alex Stamos leaves Yahoo.
2016	February	Yahoo announces the sale of its core business.
	Sometime in late July	Senior management, including Marissa Mayer, definitively learns of the 2014 data breach.
	July 25	Verizon announces $4.8 billion deal to acquire Yahoo's internet operations.
	September 9	Yahoo represents in a filing with the SEC that it knows of no cybersecurity vulnerabilities.
	September 19	Yahoo informs Verizon of 2014 data breach affecting 500 million user accounts.
	September 22	Yahoo publicly discloses the existence of the 2014 data breach.
	December 14	Yahoo publicly discloses the existence of the 2013 data breach.

260. *Id.* at 15.

2017	January 10	Yahoo announces that multiple members of the Board, including Marissa Mayer, will leave the company after the Verizon acquisition closes (assuming it does).
	January 22	The media reports that Yahoo is currently the subject of an ongoing SEC investigation regarding the timing of its breach disclosures.
	February 21	Verizon announces a renegotiated deal for Yahoo's core Internet business for $4.48 billion ($350 million less than the original price) and with an agreement the two companies will share the future cost of liability stemming from the breaches.
	March 1	Yahoo's 2016 Annual Report details the results of an internal investigation into the 2014 breach. Ronald Bell, the Company's general counsel, resigns, and CEO Marissa Mayer returns and forgoes compensation totaling $14 million.
	June 8	Yahoo shareholders vote to approve the sale of the company's Internet businesses to Verizon.

III. ANALYSIS

A. *Yahoo Breached the Duty to Provide Security, the Duty to Monitor, and the Duty to Disclose*

Before analyzing whether Yahoo's conduct between the 2014 data breach and its disclosure in September 2016 breached a corporate duty, we briefly address the overarching issue of the variety of complainants who are already asserting these claims and are likely to assert them in the future. The constituencies who have potential claims against Yahoo for conduct connected to the breach and the handling thereof is both wide and deep.

The FTC is likely to have a strong case against Yahoo for its deficient cybersecurity practices, potentially breaching its duty to provide data security.[261] We refer to any potential liability resulting from a settlement with the FTC or an adjudication in the FTC's favor as "primary liability." Primary liability stands in contrast to the possibility that a judgment in the FTC's favor may be later used by Yahoo shareholders in a derivative action against the Company's

261. *See supra* notes 193–207 and accompanying text (highlighting specific examples of Yahoo's apparent failure to enact adequate corporate cyber-security practices).

directors and officers; we refer to any potential liability stemming from a settlement or an adverse judgment against Yahoo's directors and/or officers in a derivative suit as "secondary liability."

Conversely, the duty to monitor is explicitly a duty that officers and directors owe to the corporate form and its shareholders,[262] meaning that liability stemming from a derivative action is the primary and only liability.

Finally, a breach of the duty to disclose will likely result in primary liability flowing from both enforcement action by the SEC and potential losses that Yahoo shareholders will suffer from the Verizon acquisition. Similar to the duty to provide security, Yahoo shareholders may be able to cite primary liability to the SEC and loss of Verizon value as a basis for secondary liability through a derivative action.

1. Duty to provide data security

In light of the facts related to the breach of Yahoo's security apparatus, it is exceptionally likely that the FTC will bring an enforcement action against Yahoo, contending that Yahoo's lax commitment to cybersecurity constituted an unfair trade practice.[263] Because the FTC's unfair trade practice liability theory considers a robust WISP, the gold standard for exceeding the standard needed for the duty to provide data security, this section analyzes Yahoo's cybersecurity practices against the six relevant components of WISP.[264]

Assign Responsibility. Particularly with the 2014 hiring of Alex Stamos to be Yahoo's CISO, Yahoo has appeared at times to be taking data security more seriously.[265] While hiring Mr. Stamos and empowering him to build a team committed to securing the Company's data was a step in the right direction, his departure after only sixteen months—paired with news reports regarding frequent clashes with more senior executives—suggests Yahoo's actions were skewed towards changing appearances but not the underlying

262. *See* Gould v. Am. Hawaiian S.S. Co., 331 F. Supp. 981, 999 (D. Del. 1971) (holding that directors owed a fiduciary duty to shareholders).

263. *See supra* Part II (discussing the Yahoo breach, including the facts giving rise to Yahoo's breach of its fiduciary duties to provide data security, monitor, and disclose).

264. *See supra* note 52. We do not address the seventh and final element of WISP, which addresses third party issues, because a technology company such as Yahoo has significantly fewer third party issues than, for example, a retail business utilizing a third-party vendor for online sales or a business in the service industry that relies on a third-party cloud computing service. In short, technology companies like Yahoo are prone to keep the overwhelming majority of their data and information in house.

265. *See* Perlroth & Goel, *supra* note 189 (examining Yahoo's response to its compromised cybersecurity following a series of data breaches between 2010 and 2014).

problems.[266] This example provides an instructive lesson for other companies: while hiring a seasoned and respected expert may be the right first step, proper execution of this first WISP criterion requires the company to *actually* empower the person assigned data security responsibilities to be able to put a plan in place and execute that plan. Mr. Stamos's brief tenure at Yahoo is illuminating because it suggests a corporate commitment to the appearance of assigning responsibility, but the Company's actual practices fell short of the necessary substantive changes to its data security policy.[267]

Identify Information Assets; Conduct Risk Assessment. It seems likely that Mr. Stamos and his team performed a process analogous to the second and third WISP steps to identify Yahoo's information assets and to assess its greatest risks. The insider account related by the *New York Times*, however, suggests that much of the due diligence Mr. Stamos oversaw was not prioritized or acted upon by the other members of Yahoo's senior management.[268] These WISP factors highlight the importance of doing more than simply running through the motions: not taking the security process seriously is potentially just as damaging as failing to initiate a process altogether.[269]

Select and Implement Responsive Security Controls; Monitor Effectiveness; Regularly Review the Security Program. Here, at the heart of WISP, Yahoo's senior management's failures become most obvious. The insider account of Yahoo's internal security process makes it plain that CEO Marissa Mayer (likely at the behest of other senior officers) was not simply oblivious to data security risks and the stakes of the Company's deficiencies, but she was actively resistant to assigning the necessary gravity to defraying the severity of these risks.[270] This aspect may unsurprisingly play an outsized role in the likely future FTC enforcement action against Yahoo—many companies have settled with the agency under far less damaging facts.[271] Taken together, the

---

266. *See id.*

267. *See, e.g., id.* (comparing Google's comprehensive "Never Again" cybersecurity overhaul with Yahoo's superficial cyber-security changes following the cyberattack by Chinese military hackers in 2010, which compromised both Google and Yahoo).

268. *See id.*

269. Smedinghoff, *supra* note 10, at 9–10. Rather than requiring the implementation of specific cybersecurity measures, WISP calls for a case-by-case analysis to determine whether companies are recursively assessing security risks and effectively enacting responsive and appropriate security measures.

270. *See* Perlroth & Goel, *supra* note 189.

271. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015). The FTC filed a suit against Wyndham Worldwide Corporation for unfair trade practices after hackers breached Wyndham's customer information database, stealing

frequent clashes between Mr. Stamos and other senior executives illustrate a company unable to execute the core elements of the comprehensive written information security process.[272]

While the FTC appears to have a strong case that Yahoo's cybersecurity practices constituted an unfair trade practice, the question of potential secondary liability to shareholders in a derivative action is far murkier.[273] Shareholders' potential derivative claims that Yahoo's management breached its duty to provide security are likely to face significant headwinds due to the business judgment rule. Specifically, Yahoo may convincingly argue that the corporate turnaround it was attempting to stage in the midst of the breach was inherently a risky proposition.[274] While business judgment plays no role in a determination of liability for unfair trade practices, Yahoo's management benefits from the level of deference afforded to management decisions concerning the level of security to implement and the amount of resources to invest in data security.[275]

The Company's announcement of its general counsel's resignation and its CEO's nominal compensation forfeiture strikes many observers as hollow and insufficient.[276] There can be little doubt much of the fault for the Company's failures rests at the highest echelons of management, and we believe the Company is likely to be forced to aggressively pursue settlements.

---

hundreds of thousands of customers' personal information. *See id.* In comparison, Yahoo's 2014 security breach compromised at least 500 million user accounts.

272. *See* Perlroth & Goel, *supra* note 189 (recounting Ms. Mayer's frequent disputes with Mr. Stamos over Ms. Mayer's lack of support for increased cybersecurity defenses).

273. We discuss the relationship between security and usability/profitability in significantly more detail in the conclusion, but this relationship has tangential relevance here as well.

274. *See supra* notes 193–95 and accompanying text. When Mr. Stamos began working for Yahoo in 2014, he attempted to overhaul the cybersecurity system: Stamos proposed an end-to-end encryption system that would have prevented Yahoo from accessing user message data, thus restricting Yahoo's ability to tailoring user services, and he also proposed user password reset measures that Yahoo directors feared would drive users to abandon Yahoo services.

275. *See* Omnicare, Inc. v. NCS Healthcare, Inc., 818 A.2d 914, 927 (Del. 2003). The business judgment rule is highly deferential and presumes that, "in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Id.*

276. *See* Swisher, *supra* note 211 ("The blame for the massive breach falls on Ron Bell and not where it belongs—at the top.").

2. Duty to monitor

We are still early in the process of revelations concerning the internal knowledge of the breach at Yahoo. More facts will undoubtedly be made public in the coming months, and these subsequent developments are almost certain to impact the analysis of whether Yahoo's directors and/or officers are likely to face liability in a shareholder derivative action that argues the Company's senior executives breached their duty to monitor. The corporate law duty of care centers on whether the corporate directors and officers employed a "good faith effort" to remain reasonably informed sufficient to "exercise good judgment."

But Yahoo admitted that at least some of its employees were aware of the breach in 2014, which is likely to prove extremely damaging.[277] Even if Yahoo did not ascertain the magnitude and size of the breach until much closer to the date that it finally disclosed the breach, few facts could mitigate the severity of deficiencies with Yahoo's internal data security monitoring and reporting systems. Particularly because Yahoo is a *technology* company—a business model that derives the vast majority of its revenues directly or indirectly from its user base—the fact that approximately two full years transpired between when some employees knew and when senior management remediated and disclosed strains credulity.[278] At the very least—and taking Yahoo at its word that senior management was in the dark about the breach until late July 2016[279]—two years of compartmentalized knowledge within the Company suggests that even if Yahoo's monitoring and reporting processes are not deficient in the abstract, they almost certainly were in practice. Put differently, it is possible at least some of Yahoo's mid-level employees believed that senior management did not want to know about the Company's data security deficiencies. A less charitable interpretation of the facts currently known is that senior management actively discouraged robust monitoring and reporting processes.[280]

---

277. *See* Goel, *supra* note 187 (reporting that Yahoo employees' prior knowledge of the cybersecurity breach, coupled with Yahoo's initial failure to disclose the breach, may diminish the value of Yahoo in its negotiations with Verizon).

278. *See id.*

279. *See* Murgia, Bradshaw & Lynch, *supra* note 186 (relaying that, according to internal sources at Yahoo, Ms. Mayer was not aware of the security breaches until late July 2016).

280. *See generally* Marianne Jennings & Lawrence J. Trautman, *Ethical Culture and Legal Liability: The GM Switch Crisis and Lessons in Governance*, 22 B.U. J. SCI. & TECH. L. 187 (2016) (depicting an example of the failure of critical information regarding a lethal ignition switch to gain timely disclosure and necessary corporate action).

The Company's disclosures regarding its internal investigation into the 2014 breach raise ever more questions. In its 2016 Annual Report, the Company disclosed that in "December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users but it is unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team."[281] The Company further argued, "there was [no] intentional suppression of relevant information."[282] The tension between these disclosures—which, in the Annual Report, are immediately adjacent to one another—is palpable and border on disingenuous. It is difficult to ascertain how it may be, on the one hand, "unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team," but on the other hand, perfectly clear that "there was [no] intentional suppression of relevant information."

In either event, it seems more likely than not that Yahoo's directors and/or officers either knew or should have known about the breach far sooner than they have currently admitted, likely opening them up to potential liability under their corporate duty to monitor. The remedial steps Yahoo has taken to date are thus unlikely to placate or satisfy the Company's many potential plaintiffs.

3. Duty to disclose

Finally, Yahoo is quite likely to face primary liability for a breach of the duty to disclose from one or more claimants. Directors owe a "fiduciary duty to disclose all material information" to shareholders whenever the Company voluntarily releases public information.[283] Because Yahoo did not disclose its security breaches with neither speed nor efficiency, investors may have a claim under the securities laws.

First, the SEC appears to have an exceedingly strong case in a future enforcement action against Yahoo. Even under the interpretation most favorable to Yahoo's management—that they were unaware of the 2014 breach until late July or early August 2016[284]—it is difficult to explain why the Company's CEO and

281. Yahoo 2016 10-K, *supra* note 221, at 47.

282. *Id.*

283. *See* Hamermesh, *supra* note 88, at 1091 (noting that this duty to disclose is triggered by the public release of information, regardless of whether stockholders seek action against the company).

284. *See* Murgia, Bradshaw & Lynch, *supra* note 186.

General Counsel signed an SEC filing in September 2016 that represented the Company was unaware of any exploitation of cybersecurity vulnerabilities.[285] There is very little, if any, language in the SEC's 2011 Guidance that could excuse what currently appears to be a grave misrepresentation to financial markets, Yahoo's own investors, and the SEC.[286]

With regard to secondary liability in a derivative action for penalties incurred to the SEC, shareholders have a significantly stronger claim here than they do under the Company's duty to provide security. While decisions concerning the level of security measures and the amount of resources to invest in security are likely protected by the business judgment rule,[287] a decision to convey a misrepresentation to the SEC and the public concerning the existence of a breach is difficult to justify even under a formulation of the business judgment rule so deferential as to be rendered nonexistent.

Second, Yahoo faces the loss of $350 million from the proposed renegotiated Verizon acquisition. Under the renegotiated deal, Yahoo shareholders stand to lose hundreds of millions of dollars of value due to management's cybersecurity failures, which may become the source of a shareholder derivative cause of action. But Yahoo management potentially has a strong rejoinder: in exchange for $350 million less, the Company has secured Verizon's agreement to share the cost of liabilities stemming from Yahoo's handling of the data breaches. What remains unclear at this time is whether $350 million is a bargain for Verizon's promise to share liability costs.

At present, it is difficult to speculate on shareholders' prospects for secondary liability for directors' and officers' conduct stemming from the potential loss in value of the Verizon acquisition. There are significant lingering questions about whether the $350 million discount will ultimately be offset by the liability sharing agreement. These issues should be resolved in the next few months.

That said, there are a few issues we feel comfortable opining on currently. Whether a court applies the business judgment rule to Yahoo management's decision about when to disclose the breach is likely to prove dispositive to this particular claim. On the one hand, it is conceivable a court, in a derivative action, will agree with Yahoo management that they declined to disclose the breach during

285. *See id.*

286. *See SEC CF Disclosure Guidance, supra* note 22.

287. *See* Omnicare, Inc. v. NCS Healthcare, Inc., 818 A.2d 914, 927 (Del. 2003) (suggesting that, as a highly deferential standard of judicial review, the business judgment rule presumes that directors' decisions are in the best interest of the corporation).

negotiations with Verizon out of a fear that disclosure would increase the chances that it would drive perhaps its only suitor away from the bargaining table altogether. If a court were to accept this argument and apply the business judgment rule to the disclosure decision, secondary liability to shareholders is unlikely.[288] On the other hand, if a court accepts the plaintiffs' argument that Yahoo management's failure to disclose constituted a misrepresentation that could only harm Yahoo's valuation, then shareholders are more likely to reap some secondary liability for unwarranted losses in the Verizon deal.[289] In either event, the ultimate severity of shareholder losses in the Verizon deal is certain to affect the shareholders' likelihood of success.

B. The Breach's Effect on the Putative Verizon Acquisition of Yahoo's Core Business

In early December 2016, Tim Armstrong, the Chief Executive Officer of AOL, said that he was "cautiously optimistic" that Verizon would complete its deal to acquire Yahoo's core internet business.[290] This statement, however, came after the *New York Post* reported in early October 2016 that Verizon was seeking a $1 billion discount off its original $4.8 billion offer, arguing that the hacking revelations had diminished Yahoo's value.[291] But the *Post* report maintained that "the Yahoo deal team is pushing back hard against any attempts to negotiate the price down."[292] Concerning the timing of the putative acquisition, Armstrong suggested in early December that the companies would start to work out the potential structure of their combined businesses in early 2017.[293]

---

288. *See In re* Caremark Int'l, Inc., 698 A.2d 959, 967–68 (Del. 1996) (framing an assessment of directors' affirmative actions, such as deciding not to disclose a cybersecurity breach, and focusing on the process that gave rise to the action rather than the content of the decision itself).

289. *See id.* at 967 (explaining that despite the business judgment rule's deferential standard of review, a director may be subject to liability if the court determines that the directors' decision-making process was irrational or was not a good faith effort to advance the company's best interests).

290. Robert Hackett, *AOL CEO Tim Armstrong "Optimistic" About Verizon Closing Its Yahoo Deal*, FORTUNE (Dec. 6, 2016), http://fortune.com/2016/12/06/yahoo-verizon-aol-ceo-tim-armstrong-optimistic.

291. *See* Claire Atkinson, *Verizon Wants $1B Discount on Yahoo Deal After Reports of Hacking, Spying*, N.Y. POST (Oct. 6, 2016, 6:02 PM), http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports.

292. *See id.*

293. *See* Hackett, *supra* note 290 (suggesting that Armstrong is hopeful that Ms. Mayer will remain on the executive board throughout the acquisition).

The disclosure in mid-December 2016 of the earlier, larger breach may have further complicated Verizon's putative acquisition.[294] After this most recent revelation, the *Wall Street Journal* reported that Verizon and Yahoo were close to an agreement, but the disclosure of the more recent, and even larger, hack "derailed" those efforts.[295]

Moreover, a *Bloomberg* report published the day after Yahoo announced the 2013 hack claimed that Verizon was then exploring a price cut or even an exit from the acquisition.[296] The report detailed that AOL CEO Tim Armstrong spearheaded a team focused on Yahoo's post-acquisition transition, while another, more isolated, Verizon group assessed the implications of the breach and Verizon's options.[297] Verizon General Counsel Craig Silliman was charged with preparing to either terminate the acquisition or renegotiate the sale at a lower purchase price.[298]

In December 2016, it seemed that whether Verizon chose to go through with the deal, and at what price, would be largely contingent upon Verizon's ability to avoid any future legal fallout from the Yahoo breaches.[299] Ultimately, however, it appears that Yahoo was largely victorious in the renegotiation talks: not only did Verizon get significantly less than a discount of $1 billion, Verizon also agreed to share future cyberliability costs with the remaining Yahoo entity, Altaba. How, and why, Verizon agreed to such unfavorable renegotiated terms is likely to come to light in the coming months.

C. Whether Yahoo Compensation Clawbacks Are in Order

Due to the narrow triggering criteria for initiating a clawback of Yahoo executives' compensation,[300] it seems unlikely that Yahoo's board

---

294. *See* Perlroth, *supra* note 179.

295. *See* McMillan, Knutson & Seetharaman, *supra* note 4.

296. Scott Moritz & Brian Womack, *Verizon Explores Lower Price or Even Exit from Yahoo Deal*, BLOOMBERG (Dec. 15, 2016, 11:00 AM), https://www.bloomberg.com/news/articles/2016-12-15/verizon-weighs-scrapping-yahoo-deal-on-hacking-liability (reporting that, although Verizon has said the deal still makes sense strategically, Verizon's General Counsel has placed Yahoo on notice that the security breach will have a material impact on the acquisition).

297. *Id.*

298. *Id.*

299. *Id.* ("Verizon is seeking to have Yahoo assume any lasting responsibility for the hack damage.").

300. *See* Yahoo 2015 10-K/A, *supra* note 246, at 42 (explaining that Yahoo's board may, at its discretion, decrease incentive awards for executive officers if those officers set forth an incorrect restatement of Yahoo's financial results).

will seek to undertake a clawback effort, even under the most dire factual scenarios Yahoo could confront over the next several months.

Recall that the relevant language of the clawback provision provides the following:

> In the event of a restatement of *incorrect Yahoo financial results*, . . . the Board . . . [may] seek recovery of the incremental portion of the incentive awards paid or awarded, whether in cash or equity, to our executive officers in excess of the awards that would have been paid or awarded *based on the restated financial results*.[301]

While there is a high likelihood that the SEC will penalize Yahoo in some way for seemingly misrepresenting the existence of the 2014 data breach in its September 9, 2016 filing, the clawback provision's specific focus on "incorrect Yahoo financial results" will likely mean that any clawback effort would be futile.[302] This conclusion is further bolstered by the provision's language concerning how much compensation could be clawed back in the event of a restatement of incorrect financial results: that the executives' compensation would only be reduced to reflect whatever the corrected financial results would be.[303] In other words, the Company's clawback provision incudes no punitive measures to disincentivize executives' nonfeasance or misfeasance; even if initiated, executive compensation would only be reduced by the amount equivalent to the executives' unjust enrichment for misrepresenting the Company's finances.[304]

This narrow language should give pause to many institutional investors. Such exceedingly narrow circumstances for clawing back compensation—as well as the lack of punitive corrective measures in the unlikely event that clawbacks are ever initiated—is hardly an effective means for aligning executives' incentives with the corporation's best interests. Yahoo itself provides an instructive example: the Company and its executives are facing a dizzying litany of enforcement actions, user lawsuits, derivative suits, and the loss of $350 million in a long-planned acquisition, yet these grave circumstances are almost certainly insufficient to invoke the Company's clawback provision.

The announcement of Mayer's voluntary forfeiture of a paltry $14 million in compensation should also give investors pause. Current

---

301. *Id.* (emphasis added).

302. *See id.*; *see also* Viswanatha & McMillan, *supra* note 237 (noting that the SEC has opened an investigation into the timing of Yahoo's disclosure of the breach).

303. *See* Yahoo 2015 10-K/A, *supra* note 246, at 42.

304. *See id.*

estimates put Mayer's total Yahoo compensation over the past five years—plus the payout she will receive from the Verizon deal's closure—at approximately $400 million.[305] Her $14 million forfeiture thus constitutes less than 4% of her total compensation. The Company's only remedial actions to date are the resignation of one senior executive and another senior executive forfeiting less than 4% of her total compensation. Due to how unlikely forced clawbacks are, shareholders are unlikely to require Mayer or anyone else return a significantly more exacting—and, we believe, more appropriate—amount of compensation.

CONCLUSION: THE CYBERSECURITY STANDARD OF CARE GOING FORWARD

Although teachable lessons abound, the debacle at Yahoo belies a more fundamental interplay of competing interests that many corporate directors and officers face in this day and age: the seeming zero-sum relationship between security—and thus usability—and profitability. For a technology company such as Yahoo—where the number of users and the amount of traffic are closely associated with the Company's revenue and profit, paired with the additional pressures facing a company in the midst of attempting a turnaround at the time of an unprecedented data breach—this relationship appears all the more stark.

The prospect of increased security measures and their associated downward pressure on usability (e.g., automatically resetting all users' passwords in the wake of learning about the breach), as well as shutting off additional future revenue streams (e.g., instituting end-to-end encryption would hamper the development of additional features and their ability to be tailored to individual users), run diametrically counter to increasing the Company's userbase and, thus, increased revenue and profitability.

But viewing the security of companies' electronic features—for technology and non-technology companies alike—as inversely correlated with the usability and profitability of those features fails to capture the entirety of the complex interplay between security and profitability.[306] Figure 1 is an illustration of the view Yahoo's senior management appears to have taken.

---

305. *See supra* note 244 and accompanying text.

306. *See, e.g., supra* notes 189–92 and accompanying text (outlining the stark differences in Yahoo's and Google's cybersecurity reform strategies following a 2010

Figure 1: The Zero-Sum Model of Security and Profitability

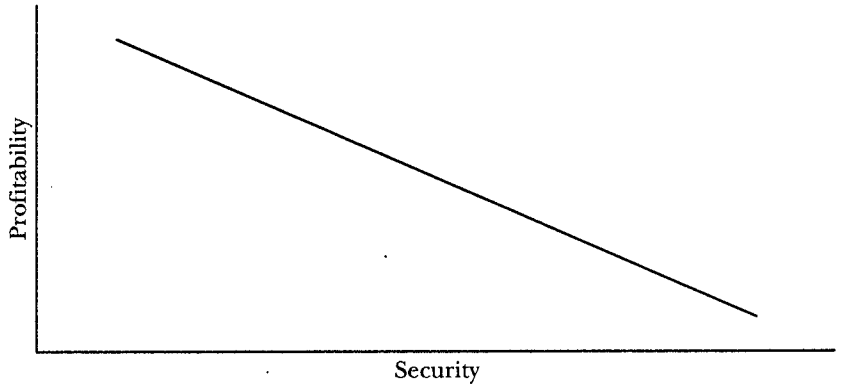
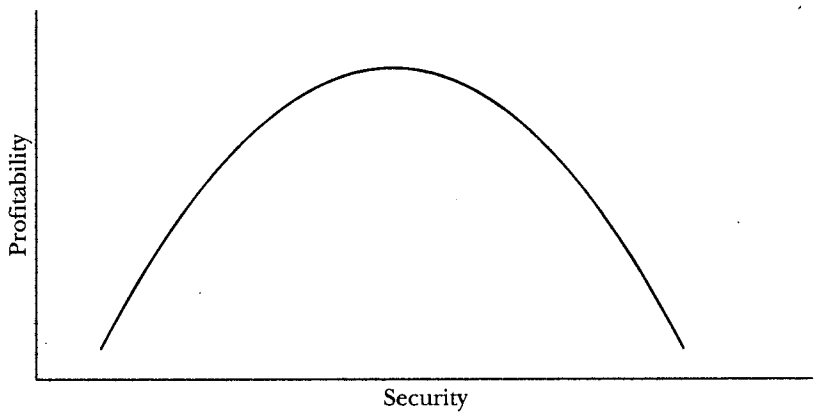


Figure 2, on the other hand, is closer to the truth.

Figure 2: The Profit-Maximizing Model of Security



While Figure 1 depicts a fully zero-sum relationship between security and profitability, Figure 2 reveals that the inverse relationship between security and profitability is only half the picture (i.e., the right half of the curve).

The relationship depicted in Figure 2 may be described as follows: at the leftmost point on the curve, a company's data security is so abysmal that not only do few, if any, users trust the company with their personal information so as to render the profitability of the

---

security breach by Chinese military hackers that compromised information of both companies).

company's electronic features a nullity, the prospect of an unfavorable judicial determination (for example, in an enforcement action by the FTC) also hampers any possibility of profits. In other words, zero security measures result in zero users and, thus, zero profitability. But, as the company's security improves, an increasing number of users trust the company with their personal information and the risk of action by the FTC decreases, both of which contribute to increased profitability. At some point—essentially, where the number of users is maximized—increased security measures begin limiting the usability of the company's electronic features and, thus, begin decreasing profitability. Taken to an extreme, excessive security measures may, theoretically, drive usability to the point of futility, rendering profit nonexistent.

It is important to note that the right half of the curve in Figure 2 is effectively identical to the relationship depicted in Figure 1: more security means less profit. The critical takeaway is that little or no digital security may be just as damaging to a company's financial health as implementing overly excessive security.

As this area of the law develops and matures in the coming years, courts, regulators, shareholders, and commentators will increasingly view the relationship between data security and corporate profitability as described in Figure 2. Perhaps the most important implication of embracing the relationship depicted in Figure 2 is that there is a profit-maximizing amount of security. And, as this view of the relationship between security and profitability is embraced, there can be little doubt that the various constituencies of stakeholders will increasingly expect corporate officers and directors to actively seek their company's profit-maximizing level of data security. If any good may come from the debacles at Yahoo, we hope it will be the advancement and clarification of corporate cybersecurity law.