ABSTRACT OF PRESENTATION:
BOARD RESPONSIBILITIES IN CYBERSECURITY

August 9, 2019

Cybersecurity remains a key concern for our increasingly digital society and economy. With each new publicly-announced breach of personal information through a computer hack, businesses are questioned increasingly as to whether they have adequate controls to prevent cyber intrusions and incident response plans to contain, remedy and mitigate any breach that may occur.

Responsibility for overseeing a corporation’s cyber-preparedness falls ultimately to its board of directors. In the US, the Securities and Exchange Commission (the “SEC”) has increased its scrutiny of publicly companies regarding their cybersecurity approach from a number of perspectives, including disclosure requirements and maintaining adequate internal controls.

The SEC issued interpretive guidance in February 2018 to assist public companies in disclosing, and crafting policies and procedures for reporting, risk management and preventing insider trading in relation to cybersecurity risks and incidents.

In October 2018, the SEC released a report of certain investigations that it had conducted regarding cyber-related frauds perpetrated against several public companies. It noted that public companies should be aware of cyber-related threats in devising and maintaining their systems of internal accounting controls and that the failure of public companies to do so in the future could lead to enforcement actions.

Toward the end of 2018, SEC Chairman Jay Clayton noted that cybersecurity was one of the three key market risks for public companies that the SEC was monitoring, and that the SEC was looking at cybersecurity from a number of perspectives. The SEC guidance provided in 2018 reinforced and expanded previous guidance provided by the SEC Division of Corporation Finance in three main areas:

- Highlighting and refining guidance on disclosure requirements that public companies must consider when evaluating cybersecurity risks and incidents;
- Emphasizing the need for disclosure controls and procedures to ensure proper disclosure of cybersecurity issues; and
- Implementing policies and procedures to prevent insider trading on, and selective disclosure of, material non-public information related to cybersecurity risks and incidents.

This increased focus on the importance of cybersecurity has several implications for U.S. public companies.

- Cybersecurity must be a priority for all companies, regardless of industry or size.
• Companies should evaluate regularly the cybersecurity risks that they face and have internal controls that are tailored to address those risks.

• Companies should evaluate regularly the adequacy of their disclosure controls and procedures, as well as their policies to protect against insider trading and selective disclosure.

• Companies should have appropriate plans in place, reviewed and tested regularly, for cyber incidents.

• Personnel responsible for cybersecurity should participate in the review and preparation of periodic reports provided to investors, and they should be included in any sub-certification and reporting processes supporting Sarbanes-Oxley certifications to be provided by the CEO and CFO.

In addition to SEC oversight, boards of directors have fiduciary obligations relating to cybersecurity under state law. These obligations consist of an oversight or monitoring role, rather than a direct role, over technology and cybersecurity, and is is based on a director’s duty to attempt in good faith to ensure that information and reporting systems exist and are adequate – a subset of the duty of loyalty. In addition to oversight and monitoring, directors also have the obligation to conduct reasonable investigation and diligence in the event of red flags or warnings. Cybersecurity should be a regular topic of discussion for the board and should include a wide array of topics to ensure that, in both appearance and substance, the board is aware of and focused on the organization’s security.
In June of 2014, then-SEC Commissioner, Luis Aguilar, counseled boards of directors that they are “already responsible for overseeing the management of all types of risks … and there can be little doubt that cyber risk also must be considered as part of the board’s overall risk oversight.”

Recent wide-scale data breaches demonstrate the catastrophic effects of boards of directors’ failure to oversee cybersecurity. Not only is there significant financial cost in responding to the breach, notifying data subjects and settling consumer and business partner litigation, but there is also significant business disruption that can halt or slow operations. Perhaps most costly, however, is the reputational harm, the negative publicity, and the loss of consumer confidence. These losses can lead to claims against directors for breach of their fiduciary duties of loyalty and care.

While cybersecurity issues are becoming increasingly prevalent, the coinciding fiduciary duties of directors have not been well defined. However, courts’ views of fiduciary duties related to cybersecurity appear to be shifting to allow greater personal liability for directors. Therefore, directors must understand their responsibilities and potential liability pertaining to cybersecurity.

1. A Director’s Fiduciary Duties

The board of directors has an oversight or monitoring role, rather than a direct role, over technology and cybersecurity within an organization. A director’s oversight role is based on a director’s duty to attempt in good faith to ensure that information and reporting systems exist and are adequate — a subset of the duty of loyalty. See In re Caremark Intl., Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996) (establishing the need for a board to monitor issues and implement monitoring programs that can detect violations); Stone v. Ritter, 911 A.2d 362 (Del. 2006) (adding to the Caremark standard that directors must exercise “good faith” in dealing with potential or actual violations of the law and corporate policy). As explained by the Delaware Supreme Court:

Caremark articulates the necessary conditions predicate for director oversight liability: (a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention. In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations. Where directors fail to act in the face of a known duty to act, thereby demonstrating a conscious disregard for their

responsibilities, they breach their duty of loyalty by failing to discharge that fiduciary obligation in good faith.

Stone, 911 A.2d at 370. Thus, to “hold directors liable for a failure in monitoring, the directors have to have acted with a state of mind consistent with a conscious decision” to breach their fiduciary duties. Desimone v. Barrows, 924 A.2d 908, 935 (Del. Ch. 2007). In light of that demanding standard, “a claim that directors are subject to personal liability for employee failures is ‘possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.’” Stone, 911 A.2d at 372 (quoting Caremark, 698 A.2d. at 967).

The Delaware Supreme Court recently clarified (and possibly expanded) the standard for Caremark claims in Marchand v. Barnhill, 2019 Del. LEXIS 310 (Del. Supr. June 19, 2019). In Marchand, the Court found that an ice cream company’s directors and executives breached their fiduciary duties of loyalty by failing to make good faith efforts to ensure that the company’s regulatory compliance programs were adequate. There, the company distributed ice cream tainted with listeria, which resulted in the deaths of three people. Plaintiffs brought derivative claims to recoup their investments alleging that the directors breached their fiduciary duties under Caremark by failing to establish a monitoring system for the company’s food safety compliance with federal and state regulatory regimes. The court determined that, while the company had regulatory compliance programs that nominally complied with FDA regulations, the complaint alleges that the company’s board “had no committee overseeing food safety, no full board-level process to address food safety issues, and no process by which the board was expected to be advised of food safety reports and developments. . . Thus, the complaint alleges specific facts that create a reasonable inference that the directors consciously failed ‘to attempt to assure reasonable information and reporting systems exist[ed].’” That constituted a failure to satisfy the duty of loyalty because the “board [must] make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation’s central compliance risks.”

As Marchand illustrates, a director’s duty of care requires not only oversight and monitoring, but also reasonable investigation and diligence in the event of red flags or warnings. Though the board’s oversight should be reasonable, perfect or exhaustive oversight is not necessary to fulfill the board’s duties. This oversight role requires directors to implement cybersecurity reporting systems and controls as well as monitor the systems and controls to remain abreast of potential risks, “red flags”, or cybersecurity threats. In fulfilling their monitoring duties, directors should also ask executives and high-level technology and cybersecurity personnel about the technology security practices and policies of the organization.

Cybersecurity should be a regular topic of discussion for the board and should include a wide array of topics to ensure that, in both appearance and substance, the board is aware of and focused on the organization’s security. The following are six topics that boards should consider for their investigation and discussion.

A. Regulatory Environment

Directors should be aware of which regulatory bodies have authority over the organization. The type of regulatory body could vary depending on whether the organization is public or private, the type of information that the organization gathers and maintains, to whom it
disseminates information, and where the organization does business. While an organization’s violation of data security regulations will not generally trigger fiduciary liability, such a violation can be a “red flag” that, if ignored by directors, could trigger personal fiduciary liability. Therefore, understanding the regulatory environment is essential to limiting director liability. Some relevant questions directors should ask executives include:

- What types of information does the organization maintain or receive?
- What laws and regulations, both national and international, govern collection and retention of this type of information?
- How does the organization interact with the information of suppliers, customers and partners? Does the organization share, receive, or store information from those parties?
- Does the organization provide information “downstream” that would affect the organization if compromised?

B. Security Culture and Policies

Establishing a culture of security by consistently updating and enforcing physical and technological security policies is essential to maintaining a safe cybersecurity posture. A “tone at the top” focused on cyber and technology security can be very effective in achieving a culture of safety and should be established by both executives and directors. Furthermore, board members should see that employees receive regular and frequent safety training, that policies are regularly updated, and that policies are properly enforced. Some relevant questions directors should ask executives include:

- Do employees receive regular cybersecurity training?
- What are the organization’s cybersecurity policies (including training manuals and formal and informal policies)?
- Who has administrator privileges and what policies govern administrator activity?
- What are the procedures for physical security, such as visitor policies, restricted area policies, and logging employees’ use of access keys?
- What are the organization’s policies relating to: email filtering, password strength and periodic password changes, USBs and other external drives or portable media (CDs, DVDs, etc.), file sharing, and employee devices used for work?

C. Information Security Roles

The board can ensure that it receives regular updates about any changes or red flags related to cybersecurity by directly communicating with the head of technology and cybersecurity. Furthermore, to maintain better oversight over cybersecurity, the board can
monitor of the number of cybersecurity employees and whether there are sufficient employees for both routine and emergency situations. The board should be aware of the parameters of its Caremark oversight duties, including knowing which members of the board have cybersecurity responsibilities. Some relevant questions directors should ask executives include:

- What executives are responsible for the organization’s cybersecurity and technology?
  - What are the parameters of their job(s)?
  - What are the checks and balances regulating the head of technology? Do any positions improperly overlap?
  - Do they have regular/direct contact with the board?

- Who is responsible for the day-to-day management of cybersecurity?
  - What are the qualifications of those individuals?
  - Who is responsible for ensuring that operating systems and other software are kept up to date with the most recent patches and revisions?
  - Does the organization have enough IT staff to handle both routine patching and technology updates, as well as emergency situations?

- What is the role of board of director oversight?
  - Who is the lead director on cybersecurity and is that position formal or informal?
  - Is at least one director sufficiently technically educated to lead board discussions and questions on information security?

- What are the greatest concerns of the people responsible for managing cybersecurity? What has been done to address those concerns?

D. Hardware and Software

While an intimate knowledge of the organization’s technology infrastructure is beyond the scope of a director’s oversight role, directors should have enough knowledge of the structure of the organization’s hardware, software, and possible vulnerability to have reasonable oversight of the firm’s technology usage. *In re Caremark Int’l., Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996). Appropriate knowledge includes a familiarity with systems used to prevent cybersecurity attacks, scan emails and websites for malicious content, and protect hard drives, computers and mainframes. Some relevant questions directors should ask executives include:

- What is the organization’s back-up procedure? How often and where are systems backed up?
• Does the organization have technology to detect, block, and remove or quarantine malware from emails, email attachments, or malicious websites?

• Are computer systems “compartmentalized” so in the event of a breach, the malware cannot extend beyond a single server?

• What does the organization’s network map look like? What data is stored on which servers?

E. Third-Party Services

Third-party services, both technological and physical, are among the greatest risks to an organization’s cybersecurity. Boards should oversee the prudent selection and monitoring of service providers to ensure that information of the organization remains free of unnecessary risk. If the organization has data breach insurance, directors should also be familiar with the insurance policies. Some relevant questions directors should ask executives include:

• How does the organization vet and monitor third-party contractors who have physical or remote access to the workplace?

• What information security functions are provided by third-parties and what is the level of assurance in the integrity of those contractors? Is there indemnification for any potential flaws?

• Does the organization have an outside cybersecurity consultant? What is their role, and how consistent is their communication with executives or the board?

• What insurance does the organization carry for data breaches and what are the policy limits and exclusions? Does the insurance cover both first- and third- party data losses?

F. Cyber Risk Assessment and Planning

Courts require boards of directors to regularly monitor cybersecurity systems. Monitoring may include a security audit conducted either through a third-party or by the organization’s Dodd-Frank-required enterprise risk committee\(^2\). Regardless of the method, regular cyber risk assessments ensure that boards are monitoring risk. However, monitoring

---

\(^2\) The Dodd-Frank Wall Street Reform and Consumer Protection Act requires publically traded banks with over $10 billion of assets to have separate risk committees comprised of independent directors. However, nonfinancial service companies often look to Dodd-Frank’s enterprise risk committees as a best practice to monitor cybersecurity and as a method to demonstrate to shareholders the level of care taken to monitor security issues. The risk committee’s roles can include identifying, managing, and monitoring risks; reporting risks to management; engaging management to discuss risk appetite; and watching for dysfunctional behavior which could lead to expectation gaps, redundancies, and cost sinks.
alone is insufficient. The board should consider deficiencies revealed in audits and adopt a security plan that is tailored to the organization’s specific risk profile. Some relevant questions directors should ask executives include:

- Does the organization regularly receive a security audit to assess security threats? If so, what does the audit assess, and who conducts the assessment?
- Does the relevant committee regularly review cybersecurity issues?
- Who are the organization’s likely adversaries who would want to access the technology? What are the geographic scope, motives, and capabilities of adversaries?
- What are the details of the organization’s cyber breach response plan? Under what circumstances will the board be notified of any cybersecurity issue?

2. Fiduciary Liability for Failure to Oversee Cybersecurity

In the past, directors were generally free from personal liability for cybersecurity breaches, because directors’ cybersecurity duties were unclear. Personal fiduciary liability claims against Wyndham, Target, and Home Depot directors were all dismissed because the directors’ cybersecurity monitoring duties were not clear enough to be “known duties” that would give rise to personal liability. Courts also concluded that claims that directors should have known of threats or had access to information about threats do not create liability for fiduciaries. However, current trends suggest that directors might be more likely to face personal liability for cybersecurity breaches in the future as directors’ cybersecurity responsibilities become clearer. See In re Equifax, Inc. Secur. Litig., 357 F. Supp. 3d 1189 (N.D. Ga. 2019) (declining to dismiss a claim against a director with personal knowledge of cybersecurity vulnerabilities); In re Yahoo! Inc. Shareholder Litig., Case No. 17-CV-307054 (Cal. Supp. Ct. Jan. 4, 2019) (approving the first settlement related to a consolidated derivative litigation for data breach brought against directors and officers). The complexity and frequency of cybersecurity breaches, the severe consequences of a breach to corporations, and the growth of the cybersecurity industry all appear to clarify directors’ cybersecurity duties. When directors fail to institute or monitor cybersecurity measures, or when they consciously disregard red flags that they have a known duty to address, shareholders may bring claims to hold directors personally liable. Recently, a court declined to dismiss a claim against the CEO of Equifax who, despite having personal knowledge of organization’s cybersecurity vulnerabilities, misrepresented the strength of the organization’s technology. In re Equifax, Inc. Secur. Litig., 357 F. Supp. 3d 1189 (N.D. Ga. 2019) (CEO’s personal knowledge of the breach, known duty to act on the knowledge, and refusal to address the issue exposed him to personal liability).

3. Conclusion

Directors have a duty to oversee an organization’s management of its cybersecurity risks. Instituting, updating, and monitoring system controls is key to avoiding personal fiduciary liability, and directors should give special attention to any red or yellow flags. As cybersecurity
threats continue to proliferate, directors’ good faith efforts to fulfill their oversight duties will not only protect them from potential personal liability, it will also protect the organization, its customers, employees, and shareholders.

**ADDITIONAL READING**


IN THE SUPREME COURT OF THE STATE OF DELAWARE

JACK L. MARCHAND II, §
   Plaintiff Below, §
   Appellant, §
   §
   v. §
   §
   JOHN W. BARNHILL, JR., GREG §
   BRIDGES, RICHARD DICKSON, §
   PAUL A. EHLERT, JIM E. KRUSE, §
   PAUL W. KRUSE, W.J. RANKIN, §
   HOWARD W. KRUSE, PATRICIA §
   I. RYAN, DOROTHY MCLEOD §
   MACINERNEY and BLUE BELL §
   CREAMERIES USA, INC., §
   §
   Defendants Below, §
   Appellee. §

   §

   Submitted: April 24, 2019
   Decided: June 18, 2019

Before STRINE, Chief Justice; VALIHURA, VAUGHN, SEITZ, and TRAYNOR, Justices, constituting the Court en Banc.

Upon appeal from the Court of Chancery. REVERSED and REMANDED.

Robert J. Kriner, Jr., Esquire (Argued), and Vera G. Belger, Esquire, CHIMICLES & TIKELLIS LLP, Wilmington, Delaware; Michael Hawash, Esquire, and Jourdain Poupore, Esquire, HAWASH CICACK & GASTON LLP, Houston, Texas, Attorneys for Appellant, Jack L. Marchand II.

Paul A. Fioravanti, Jr., Esquire (Argued), and John G. Day, Esquire, PRICKETT, JONES & ELLIOT, P.A., Wilmington, Delaware, Attorneys for Appellees, John W. Barnhill, Jr., Richard Dickson, Paul A. Ehlert, Jim E. Kruse, W.J. Rankin, Howard W. Kruse, Patricia I. Ryan, Dorothy McLeod MacInerney, and nominal defendant Blue Bell Creameries USA, Inc.

STRINE, Chief Justice:
Blue Bell Creameries USA, Inc., one of the country’s largest ice cream manufacturers, suffered a listeria outbreak in early 2015, causing the company to recall all of its products, shut down production at all of its plants, and lay off over a third of its workforce. Blue Bell’s failure to contain listeria’s spread in its manufacturing plants caused listeria to be present in its products and had sad consequences. Three people died as a result of the listeria outbreak. Less consequentially, but nonetheless important for this litigation, stockholders also suffered losses because, after the operational shutdown, Blue Bell suffered a liquidity crisis that forced it to accept a dilutive private equity investment.

Based on these unfortunate events, a stockholder brought a derivative suit against two key executives and against Blue Bell’s directors claiming breaches of the defendants’ fiduciary duties. The complaint alleges that the executives—Paul Kruse, the President and CEO, and Greg Bridges, the Vice President of Operations—breached their duties of care and loyalty by knowingly disregarding contamination risks and failing to oversee the safety of Blue Bell’s food-making operations, and that the directors breached their duty of loyalty under Caremark.¹

The defendants moved to dismiss the complaint for failure to plead demand futility.\(^2\) The Court of Chancery granted the motion as to both claims. As to the claim against management, the Court of Chancery held that the plaintiff “failed to plead particularized facts that raise a reasonable doubt as to whether a majority of [Blue Bell’s] Board could impartially consider a demand.”\(^3\) Although the complaint alleged facts sufficient to raise a reasonable doubt as to the impartiality of a number of Blue Bell’s directors, the plaintiff ultimately came up one short in the Court of Chancery’s judgment: the plaintiff needed eight directors for a majority, but only had seven.

As to the Caremark claim, the Court of Chancery held that the plaintiff did not plead any facts to support “his contention that the [Blue Bell] Board ‘utterly’ failed to adopt or implement any reporting and compliance systems.”\(^4\) Although the plaintiff argued that Blue Bell’s board had no supervisory structure in place to oversee “health, safety and sanitation controls and compliance,” the Court of Chancery reasoned that “[w]hat Plaintiff really attempts to challenge is not the existence of monitoring and reporting controls, but the effectiveness of monitoring

\(^2\) App. to Answering Br. at B48–134 (Defendants’ Opening Br. in Support of their Joint Motion to Dismiss (Oct. 30, 2017)); see also Court of Chancery Rule 23.1.


\(^4\) Id. at *18.
and reporting controls in particular instances,” and “[t]his is not a valid theory under . . . Caremark.”

In this opinion, we reverse as to both holdings.

We first hold that the complaint pleads particularized facts sufficient to create a reasonable doubt that an additional director, W.J. Rankin, could act impartially in deciding to sue Paul Kruse, Blue Bell’s CEO, and his subordinate Greg Bridges, Blue Bell’s Vice President of Operations, due to Rankin’s longstanding business affiliation and personal relationship with the Kruse family. According to the complaint, Rankin worked at Blue Bell for decades and owes his entire career to Ed Kruse, the current CEO’s father, who hired Rankin as his administrative assistant in 1981 and promoted him five years later to the position of CFO, a position Rankin maintained until his retirement in 2014. In 2004, while serving as CFO, Rankin was elected to Blue Bell’s board, and has served since then. Moreover, the complaint alleges that the Kruse family showed its appreciation for Rankin not only by supporting his career, but also by leading a campaign that raised over $450,000 to name a building at the local university after Rankin. Despite the defendants’ contentions that Rankin’s relationship with the Kruse family was just an ordinary

---

5 Id.
6 Because we hold that the complaint pleads particularized facts supporting a reasonable inference that Rankin could not be impartial as to suing a member of the Kruse family, we need not, and do not, reach that issue as to the other director whose impartiality the plaintiff challenges on appeal.
business relationship from which Rankin would derive no strong feelings of loyalty toward the Kruse family, these allegations are “suggestive of the type of very close personal [or professional] relationship that, like family ties, one would expect to heavily influence a human’s ability to exercise impartial judgment.”

Rankin’s apparently deep business and personal ties to the Kruse family raise a reasonable doubt as to whether Rankin could “impartially or objectively assess whether to bring a lawsuit against the sued party.”

As to the Caremark claim, we hold that the complaint alleges particularized facts that support a reasonable inference that the Blue Bell board failed to implement any system to monitor Blue Bell’s food safety performance or compliance. Under Caremark and this Court’s opinion in Stone v. Ritter, directors have a duty “to exercise oversight” and to monitor the corporation’s operational viability, legal compliance, and financial performance. A board’s “utter failure to attempt to assure a reasonable information and reporting system exists” is an act of bad faith in breach of the duty of loyalty.

---

8 In re Oracle Corp. Derivative Litig., 824 A.2d 917, 942 (Del. Ch. 2003).
9 911 A.2d 362 (Del. 2006).
10 Id. at 364 (quoting In re Caremark Int’l Inc. Derivative Litig., 698 A.2d 959, 971 (Del. Ch.1996)); see also In re Citigroup Inc. S’holder Derivative Litig., 964 A.2d 106, 125 (Del. Ch. 2009) (Chandler, C.).
11 Caremark, 698 A.2d at 971.
As a monoline company that makes a single product—ice cream—Blue Bell can only thrive if its consumers enjoyed its products and were confident that its products were safe to eat. That is, one of Blue Bell’s central compliance issues is food safety. Despite this fact, the complaint alleges that Blue Bell’s board had no committee overseeing food safety, no full board-level process to address food safety issues, and no protocol by which the board was expected to be advised of food safety reports and developments. Consistent with this dearth of any board-level effort at monitoring, the complaint pleads particular facts supporting an inference that during a crucial period when yellow and red flags about food safety were presented to management, there was no equivalent reporting to the board and the board was not presented with any material information about food safety. Thus, the complaint alleges specific facts that create a reasonable inference that the directors consciously failed “to attempt to assure a reasonable information and reporting system exist[ed].”\textsuperscript{12}

\textsuperscript{12} \textit{Id.}
I. Background

A. Blue Bell’s History and Operating Environment

i. History

Founded in 1907 in Brenham, Texas, Blue Bell Creameries USA, Inc. (“Blue Bell”), a Delaware corporation, produces and distributes ice cream under the Blue Bell banner. By 1919, Blue Bell’s predecessor was struggling financially. Blue Bell’s board turned to E.F. Kruse, who took over the company that year and turned it around. Under his leadership, the company expanded and became profitable.

E.F. Kruse led the company until his unexpected death in 1951. Upon his death, his sons, Ed F. Kruse and Howard Kruse, took over the company’s management. Rapid expansion continued under Ed and Howard’s leadership.

13 The facts come from the plaintiff’s complaint, documents incorporated by reference into the complaint, and the Court of Chancery’s opinion based on these same documents.
14 Blue Bell Creameries USA, Inc. is a holding company. Its only assets are a 69.6 percent interest in Blue Bell Creameries, L.P., which actually produces and distributes ice cream, and a 100 percent interest in Blue Bell Creameries, Inc., the general partner of Blue Bell Creameries, L.P. Because the plaintiff is a stockholder of Blue Bell Creameries USA, the Court of Chancery requested supplemental briefing regarding the fiduciary duties of dual fiduciaries—because the holding company and the general partner have the same executives—and a board’s responsibilities when its only asset is a majority stake in a subsidiary. App. to Opening Br. at A275–83 (Letter from Vice Chancellor Slichts to counsel requesting supplement submissions (May 11, 2018)). But in its decision, the Court of Chancery sensibly and properly collapsed the enterprise for purposes of analyzing the complaint. Marchand v. Barnhill, 2018 WL 4657159, at *3 (Del. Ch. Sept. 27, 2018).
15 App. to Opening Br. at A20 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
16 Id. at A20–21.
17 Id. at A21.
2004, Ed Kruse’s son, Paul Kruse, took over management, becoming Blue Bell’s President and CEO. Ten years later, in 2014, Paul Kruse also assumed the position of Chairman of the Board, taking the position from his retiring father.

**ii. The Regulated Nature of Blue Bell’s Industry**

As a U.S. food manufacturer, Blue Bell operates in a heavily regulated industry. Under federal law, the Food and Drug Administration (“FDA”) may set food quality standards, require food manufacturing facilities to register with the FDA, prohibit regulated manufacturers from placing adulterated food into interstate commerce, and hold companies liable if they place any adulterated foods into interstate commerce in violation of FDA rules. Blue Bell is “required to comply with regulations and establish controls to monitor for, avoid and remediate contamination and conditions that expose the Company and its products to the risk of contamination.”

Specifically, FDA regulations require food manufacturers to conduct operations “with adequate sanitation principles” and, in line with that obligation, “must prepare . . . and implement a written food safety plan.” As part of a

---

18 *Id.* at A28–29.
19 *Id.*
21 App. to Opening Br. at A28 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
22 21 C.F.R. § 110.80.
23 *Id.* § 117.3.
manufacturer’s food safety plan, the manufacturer must include processes for conducting a hazard analysis that identifies possible food safety hazards, identifies and implements preventative controls to limit potential food hazards, implements process controls, implements sanitation controls, and monitors these preventative controls. Appropriate corporate officials must monitor these preventative controls.\textsuperscript{24}

Not only is Blue Bell subject to federal regulations, but it must also adhere to various state regulations. At the time of the\emph{listeria} outbreak, Blue Bell operated in three states, and each had issued rules and regulations regarding the proper handling and production of food to ensure food safety.\textsuperscript{25}

\textit{B. Plaintiff’s Complaint}

With that context out of the way, we briefly summarize the plaintiff’s well-pled factual allegations and the reasonable inferences drawn from them.

The complaint starts by observing that, as a single-product food company, food safety is of obvious importance to Blue Bell.\textsuperscript{26} But despite the critical nature of food safety for Blue Bell’s continued success, the complaint alleges that management turned a blind eye to red and yellow flags that were waved in front of it by regulators and its own tests, and the board—by failing to implement any system

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{24} \textit{Marchand v. Barnhill}, 2018 WL 4657159, at *9–11 (Del. Ch. Sept. 27, 2018).
\item \textsuperscript{25} \textit{Id}.
\item \textsuperscript{26} App. to Opening Br. at A9 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017))
\end{itemize}
\end{footnotesize}
to monitor the company’s food safety compliance programs—was unaware of any problems until it was too late.27

i. The Run-Up to the Listeria Outbreak

According to the complaint, Blue Bell’s issues began to emerge in 2009. At that time, Paul Kruse, Blue Bell’s President and CEO, and his cousin, Paul Bridges, were responsible for the three plants Blue Bell operated in Texas, Oklahoma, and Alabama.28 The complaint alleges that, despite being responsible for overseeing plant operations, Paul Kruse and Bridges failed to respond to signs of trouble in the run up to the listeria outbreak. From 2009 to 2013 several regulators found troubling compliance failures at Blue Bell’s facilities:

- In July 2009, the FDA’s inspection of the Texas facility revealed “two instances of condensation, one from a pipe carrying liquid caramel [that] was dripping into three gallon cartons waiting to be filled, and one dripping into ice cream sandwich wafers.”29 The FDA reported these observations directly to Paul Kruse, who assured the FDA that “condensation is treated by Blue Bell as a serious concern.”30

- In March 2010, the Alabama Department of Health inspected the Alabama plant and “found equipment left on the floor and a ceiling in disrepair in the container forming room.”31

- Two months later, in May 2010, the FDA returned to the Texas plant “and observed ten violations that were cited to Paul Kruse

27 Id. at A9–11.
28 Id. at A21.
29 Id. at A25.
30 Id. at A33.
31 Id.
including, again, a condensation drip.”\textsuperscript{32} While the condensation drip persisted from the FDA’s last inspection of the Texas plant, the FDA also observed “ripped and open containers of ingredients, inconsistent hand-washing and glove use and a spider and its web near the ingredients.”\textsuperscript{33}

- In July 2011, an inspection by “the Alabama Department of Public Health cited drips from a ceiling unit and pipelines, standing water, open tank lids and unprotected measuring cups.”\textsuperscript{34}

- Nine months later, in March 2012, an inspection of the Oklahoma facility revealed the plant’s “[f]ailure to manufacture foods under conditions and controls necessary to minimize contamination’ and ‘[f]ailure to handle and maintain equipment, containers and utensils used to hold food in [sic] manner that protects against contamination.”\textsuperscript{35}

- That same month, in March 2012, “[t]he Alabama Department of Public Health required five changes” to the Alabama facility, “including instructions to clean various rooms and items, make repairs and [sic] after fruit processing to prevent contamination.”\textsuperscript{36} A year later, “in March 2013, the Alabama Department of Public Health again ordered cleaning and repairs and observed an uncapped fruit tank.”\textsuperscript{37} The Alabama Department of Public Health made similar observations in a July 2014 inspection.\textsuperscript{38}

Regulatory inspections during this time were not the only signal that Blue Bell faced potential health safety risks. In 2013, “the Company had five positive tests”

\textsuperscript{32} Id.
\textsuperscript{33} Id. at A34.
\textsuperscript{34} Id.
\textsuperscript{35} Id.
\textsuperscript{36} Id.
\textsuperscript{37} Id.
\textsuperscript{38} Id.
for *listeria*, and in January 2014, “the Company received a presumptive positive *listeria* result reports from the third party laboratory for the [Oklahoma] facility on January 20, 2014 and the samples reported positive for a second time on January 24, 2014.”

Although management had received reports about *listeria*’s growing presence in Blue Bell’s plants, the complaint alleges that the board never received any information about *listeria* or more generally about food safety issues. Minutes from the board’s January 29, 2014 meeting “reflect no report or discussion of the increasingly frequent positive tests that had been occurring since 2013 or the third party lab reports received in the preceding two weeks.” Board meeting minutes from February and March likewise reflect no board-level discussion of *listeria*.

During the rest of 2014, Blue Bell’s problems accelerated, but the board remained uninformed about Blue Bell’s problems. In April, “[t]he Company received further positive *listeria* lab tests regarding [the Oklahoma facility].” That same month, the company had three “positive coliform tests far above the known legal regulator limits.” Yet, minutes from the April board meeting reflected

---

39 *Id.* at A49–50.
40 *Id.* at A52.
41 *Id.*
42 *Id.* (“[T]here is no reference to *Listeria* or the lab reports in the minutes of the February or March 2014 meetings.”).
43 *Id.*
44 *Id.* at A49–50.
no discussion of *listeria*. Instead, the minutes note only that the Oklahoma and Alabama facilities’ “plant operations were discussed briefly” and that Bridges also discussed “a good report from the TCEQ [Texas Commission on Environmental Quality].”45

Over the course of 2014, Blue Bell received ten positive tests for *listeria*. According to the complaint, these positive tests “included repeated positive results from the Company’s third party laboratory in 2014, on consecutive samples, evidencing the inadequacy of the Company’s remedial methods to eliminate the contamination.”46

Despite management’s knowledge of the growing problem, the complaint alleges that this information never made its way to the board, and the board continued to be uninformed about (and thus unaware of) the problem. Minutes from the board’s 2014 meetings are bereft of reports on the *listeria* issues. Only during the September meeting is sanitation discussed, when Bridges informed the board that “[t]he recent Silliker audit [Blue Bell’s third-party auditor for sanitation issues in 2014] went well.”47 This lone reference to a third-party audit is the only instance,

---

45 *Id.* at A170 (Minutes to April 29, 2014 board meeting).
46 *Id.* at A49 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
47 *Id.* at A180 (Minutes to September 30, 2014 board meeting). *See also Marchand*, 2018 WL 4657159, at *6 n.72.
until the *listeria* outbreak forced the recall of Blue Bell’s products, of *any* board-level discussion regarding food safety.

At this stage of the case, we are bound to draw all fair inferences in the plaintiff’s favor from the well-pled facts. Based on this chronology of events, the plaintiffs have fairly pled that:

- Blue Bell had no board committee charged with monitoring food safety;
- Blue Bell’s full board did not have a process where a portion of the board’s meetings each year, for example either quarterly or biannually, were specifically devoted to food safety compliance; and
- The Blue Bell board did not have a protocol requiring or have any expectation that management would deliver key food safety compliance reports or summaries of these reports to the board on a consistent and mandatory basis. In fact, it is inferable that there was no expectation of reporting to the board of any kind.

In short, the complaint pleads that the Blue Bell board had made no effort at all to implement a board-level system of mandatory reporting of any kind.

*ii. The Listeria Outbreak and the Board’s Response*

Blue Bell’s *listeria* problem spread in 2015. Starting in January 2015, one of Blue Bell’s product tests had positive coliform levels above legal limits.\(^{48}\) The same

---

\(^{48}\) App. to Opening Br. at A49–50 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
result appeared in February 2015.\textsuperscript{49} And by this point, the problem spread to Blue Bell’s products and spiraled out of control.

On February 13, 2015, “Blue Bell received notification that the Texas Department of State Health Services also had positive tests for \textit{listeria} in Blue Bell samples.”\textsuperscript{50} The Texas Department of State Health Services was alerted to these positive tests by the South Carolina Health Department.\textsuperscript{51} Company swabs at the Texas facility on February 19 and 21, 2015 tested positive for \textit{listeria}.\textsuperscript{52} Yet despite these reports to management, Blue Bell’s board was not informed by management about the severe problem. The board met on February 19, 2015, following Blue Bell’s annual stockholders meeting, but there was no \textit{listeria} discussion.\textsuperscript{53}

Four days later, Blue Bell initiated a limited recall.\textsuperscript{54} Two days after that, Blue Bell’s board met, and Bridges reported that “[t]he FDA is working with Texas health inspectors regarding the Company’s recent recall of products. More information is developing and should be known within the next days or weeks.”\textsuperscript{55} Despite two years of evidence that \textit{listeria} was a growing problem for Blue Bell, this is the first time the board discussed the issue, according to the complaint and the

\textsuperscript{49} Id.
\textsuperscript{50} Id. at A36, A54.
\textsuperscript{51} Id. at A54–55.
\textsuperscript{52} Id.
\textsuperscript{53} Id. at A55.
\textsuperscript{55} App. to Opening Br. at A55 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
incorporated board minutes. Instead of holding more frequent emergency board meetings to receive constant updates on the troubling fact that life-threatening bacteria was found in its products, Blue Bell’s board left the company’s response to management.

And the problem got worse, with awful effects. “In early March 2015, health authorities reported that they suspected a connection between human [l]isteria infections in Kansas and products made by Blue Bell’s [Texas] facility.”56 The outbreak in Kansas matched a listeria strain found in Blue Bell’s products in South Carolina. And by March 23, 2015, Blue Bell was forced to recall more products. Two days later, Blue Bell’s board met and adopted a resolution “express[ing] support for Blue Bell’s CEO, management, and employees and encourag[ing] them to ensure that everything Blue Bell manufacture[s] and distributes is a wholesome and good testing [sic] product that our consumers deserve and expect.”57

Blue Bell expanded the recall two weeks later, and less than a month later, on April 20, 2015, Blue Bell “instituted a recall of all products.”58 By this point, the Center for Disease Controls and Prevention (‘‘CDC’’) had begun an investigation and discovered that the source of the listeria outbreak in Kansas was caused by Blue

56 Id. at A36.
57 Id. at A56–57.
58 Id. at A37.
Bell’s Texas and Oklahoma plants. Ultimately, five adults in Kansas and three adults in Texas were sickened by Blue Bell’s products; three of the five Kansas adults died because of complications due to *listeria* infection. The CDC issued a recall to grocers and retailers, alerting them to the contamination and warning them against selling the products.

After Blue Bell’s full product recall, the FDA inspected each of the company’s three plants. Each was found to have major deficiencies. In the Texas plant, the FDA found a “failure to manufacture foods under conditions and controls necessary to minimize the potential for growth of microorganisms,” inadequate cleaning and sanitizing procedures, “failure to maintain buildings in repair sufficient to prevent food from coming [sic] adulterated,” and improper construction of the building that failed to prevent condensation from occurring. Likewise, at the Oklahoma facility, “[t]he FDA found that the Company had been receiving increasingly frequent positive [*listeria* tests at [the Oklahoma facility] for over three years,” failed “to manufacture and package foods under conditions and controls necessary to minimize the potential growth of microorganisms and contamination,” failed to perform testing to ferret out microbial growth, implemented inadequate cleaning and

---

59 Id. at A37–38.
60 Id. at A37.
61 Id.
62 Id. at A38; see also id. at A77–80 (Food and Drug Administration Inspection Report for Blue Bell Creameries facility in Brenham, Texas (May 1, 2015)).
sterilization procedures, failed to provide running water at an appropriate
temperature to sanitize equipment, and failed to store food in clean and sanitized
portable equipment.\textsuperscript{63}

Although the Alabama facility fared better, the FDA still found contamination
and several issues, including the “failure to perform microbial testing where
necessary to identify possible food contamination,” “failure to maintain food contact
surfaces to protect food from contamination by any source,” and inadequate
construction of the facility such that condensation was likely.\textsuperscript{64} Most of these
findings, the complaint alleges, are unsurprising because similar deficiencies were
found by the FDA and state regulators in the run up to the\textit{listeria} outbreak, yet
according to the FDA’s inspection after the fact, it appeared that neither management
nor the board made progress on remedying these deficiencies.

After the fact, various news outlets interviewed former Blue Bell employees
who “claimed that Company management ignored complaints about factory
conditions in [the Texas facility].”\textsuperscript{65} One former employee “reported [that] spilled
ice cream was left to pool on the floor, ‘creating an environment where bacteria

\textsuperscript{63} Id. at A38–39 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)); \textit{see also} id.
at A82–91 (Food and Drug Administration Inspection Record for Blue Bell Creameries facility in
Broken Arrow, Oklahoma (Apr. 23, 2015)).
\textsuperscript{64} Id. at A40–41 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)); \textit{see also} id.
at A94–96 (Food and Drug Administration Inspection Report for Blue Bell Creameries facility in
Sylacauga, Alabama (Apr. 30, 2015)).
\textsuperscript{65} Id. at A35 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
Another former employee described being “instructed to pour ice cream and fruit that dripped off his machine into mix to be used later.”

iii. The Aftermath of the Listeria Outbreak

With its operations shuttered, Blue Bell faced a liquidity crisis. Blue Bell initially sought a more traditional credit facility to bridge its liquidity, but after Blue Bell director W.J. Rankin informed his brother-in-law, Bill Reimann, about Blue Bell’s liquidity crunch, Blue Bell ended up striking a deal with Moo Partners, a fund controlled by Sid Bass and affiliated with Reimann. Moo Partners provided Blue Bell with a $125 million credit facility and purchased a $100 million warrant to acquire 42% of Blue Bell at $50,000 per share. As part of Moo Partners’s investment conditions, Blue Bell also amended its certificate of incorporation to grant Moo the right to appoint one member of Blue Bell’s board who would be entitled to one-third of the board’s voting power (or five votes based on a then-10-member board).

After investing in Blue Bell, Moo named Reimann to Blue Bell’s board, expanding the board to 11 members with Reimann possessing five votes. In February 2016, Reimann suggested that the board separate the roles of CEO and

---

66 Id.
67 Id. at A35–36.
68 Id. at A42–43.
69 Id.
70 Id. at A46.
Chairman (both held by Paul Kruse). The board voted to follow Reimann’s recommendation at its February 18th meeting, but after Paul Kruse disagreed with the recommendation and threatened to resign as President and CEO if the split occurred, the board held another vote in which all members, except Reimann and Rankin, voted to restore the position of CEO and Chairman of the board.\footnote{Id. at A57–59.}

\textbf{C. The Court of Chancery Dismisses the Case}

After requesting Blue Bell’s books and records through a § 220 request, the plaintiff, a Blue Bell stockholder, sued Blue Bell’s management and board derivatively, asserting two claims based on management’s alleged failure to respond appropriately to the red and yellow flags about growing food safety issues and the board’s violation of its duty of loyalty, under \textit{Caremark}, by failing to implement any reporting system and therefore failing to inform itself about Blue Bell’s food safety compliance. The Court of Chancery dismissed both claims, holding that the plaintiff failed to plead demand futility.

As to the first claim, the plaintiff alleges that Paul Kruse, Blue Bell’s President and CEO, and Bridges, Blue Bell’s Vice President of Operations, had breached their duties of loyalty and care by knowingly disregarding contamination risks and failing to oversee Blue Bell’s operations and food safety compliance process.\footnote{Id. at A67 (asserting a “derivative claim for breach of fiduciary duties of loyalty and care for knowingly disregard of contamination [sic] risks and failure to oversee Blue Bell’s operation and compliance”).} “Because
directors are empowered to manage, or direct the management of, the business and affairs of the corporation,” the plaintiff’s complaint must allege facts suggesting that “demand is excused because the directors are incapable of making an impartial decision regarding such litigation.” The plaintiff’s complaint claims that “[a] demand upon the Board of the Company to pursue claims against Paul Kruse and Bridges . . . would be futile” because “the Kruse family—of which both Paul Kruse and Bridges are members—ha[s] long dominated Blue Bell” and the majority of directors are “long-time employees and/or otherwise beholden and loyal to the Kruse family.”

But the Court of Chancery held that the plaintiff “failed to plead particularized facts to raise a reasonable doubt that a majority of the [Blue Bell board] members could have impartially considered a pre-suit demand.” Without belaboring the details of the Court of Chancery’s thorough analysis, which is somewhat complicated due to the unusual structure of Blue Bell’s board, we note that the court essentially ruled that the plaintiff came up one vote short. To survive the Rule 23.1 motion to dismiss, the complaint needed to allege particularized facts raising a reasonable doubt that directors holding eight of the 15 votes could have impartially

74 App. to Opening Br. at A62 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
considered a demand, but the court held that the plaintiff had done so for directors holding only seven votes.

One of the directors who the trial court held could consider demand impartially was Rankin, Blue Bell’s recently retired former CFO. Although Rankin worked at Blue Bell for 28 years, the court emphasized that he was no longer employed by Blue Bell, having retired in 2014. As to the allegations that donations from the Kruse family resulted in a building at Blinn College being named for Rankin, the court noted that “the Complaint provide[d] no more specifics regarding the donation (i.e., who gave how much), and ma[de] no attempt to characterize the materiality of the gesture.”\textsuperscript{76} That failure, the Court of Chancery concluded, fell short of Rule 23.1’s particularity requirement. Further, the court noted that Rankin voted against rescinding a board initiative to split the CEO and Chairman positions held by Paul Kruse.\textsuperscript{77} In the court’s view, that act was evidence that Rankin was not beholden to the Kruse family. Ultimately, the Court of Chancery concluded that the plaintiff’s “allegation that Rankin lacks independence falls flat.”\textsuperscript{78}

The Court of Chancery also rejected the plaintiff’s second claim that Blue Bell’s directors breached their duty of loyalty under \textit{Caremark} by failing to “institute

\textsuperscript{76} \textit{Id.} at *15.
\textsuperscript{77} \textit{Id.}
\textsuperscript{78} \textit{Id.}
a system of controls and reporting” regarding food safety.

In support of this claim, the plaintiff asserted, based on the facts alleged in the complaint and reasonable inferences from those facts, that: (1) the Blue Bell board had no committee overseeing food safety; (2) Blue Bell’s board did not have any reporting system in place about food safety; (3) management knew about the growing listeria issues but did not report those issues to the board, further evidence that the board had no food safety reporting system in place; and (4) the board did not discuss food safety at its regular board meetings.

Rejecting the plaintiff’s Caremark claim, the Vice Chancellor started by observing that “[d]espite the far-reaching regulatory schemes that governed Blue Bell’s operations at the time of the [l]isteria contamination, the Complaint contains no allegations that Blue Bell failed to implement the monitoring and reporting systems required by the FDCA [Federal Food, Drug, and Cosmetic Act], FDA regulations or state statutes (or that it was ever cited for such a failure).” In fact, the Court of Chancery concluded that “documents incorporated by reference in the Complaint reveal that Blue Bell distributed a sanitation manual with standard operating and reporting procedures, and promulgated written procedures for

---

79 App. to Opening Br. at A68–69 (Verified Stockholder Derivative Action Complaint (Aug. 14, 2017)).
80 Marchand, 2018 WL 4657159, at *11.
processing and reporting consumer complaints.”81 And at the board level, the Vice Chancellor noted that “[b]oth Bridges and Paul Kruse . . . provided regular reports regarding Blue Bell operations to the . . . Board,” including reports about audits of Blue Bell’s facilities.82

Based on Blue Bell’s compliance with FDA regulations, ongoing third-party monitoring for contamination, and consistent reporting by senior management to Blue Bell’s board on operations, the Court of Chancery concluded that there was a monitoring system in place. At bottom, the Court of Chancery opined that “[w]hat Plaintiff really attempts to challenge is not the existence of monitoring and reporting controls, but the effectiveness of monitoring and reporting controls in particular instances.”83 That, the Court of Chancery held, does not state a Caremark claim. As a result, the court held that demand was not excused as to the Caremark claims and dismissed the complaint.

The plaintiff timely appealed from that dismissal.

---

81 Id. at *17.
82 Id.
83 Id. at *18 (emphasis in original).
II. Analysis

We review a motion to dismiss for failure to plead demand futility \textit{de novo}.\footnote{Beam ex rel. Martha Stewart Living Omnimedia, Inc. v. Stewart, 845 A.2d 1040, 1048 (Del. 2004) ("This Court reviews de novo a decision of the Court of Chancery to dismiss a derivative suit under Rule 23.1.").}

\textit{A. Rankin’s Independence}

We first address the plaintiff’s claim that the Court of Chancery erred by holding that the complaint did not allege particularized facts that raise a reasonable doubt as to whether directors holding a majority of the board’s votes could impartially consider demand as to the management claims. The Court of Chancery concluded that four directors representing eight votes were independent and that seven directors representing seven votes were not independent. On appeal, the plaintiff challenges the Court of Chancery’s conclusion as to only Rankin and one other director, Paul Ehlert. Holding that the Court of Chancery erred as to either director would be dispositive. Because we hold that Rankin was not independent for demand futility purposes, we reverse and need not and do not address whether Ehlert was independent.

On appeal, both parties agree that the \textit{Rales} standard applies,\footnote{See Rales v. Blasband, 634 A.2d 927, 932–34 (Del. 1993).} and we therefore use it to determine whether the Court of Chancery erred in finding that a majority of the board was independent for pleading stage purposes. “[A] lack of
independence turns on ‘whether the plaintiffs have pled facts from which the
director’s ability to act impartially on a matter important to the interested party can
be doubted because that director may feel either subject to the interested party’s
dominion or beholden to that interested party.’”86 When it comes to life’s more
intimate relationships concerning friendship and family, our law cannot “ignore the
social nature of humans” or that they are motivated by things other than money, such
as “love, friendship, and collegiality.”87

The standard for conducting this inquiry at the demand futility stage is well
balanced, requiring that the plaintiff plead facts with particularity, but also requiring
that this Court draw all reasonable inferences in the plaintiff’s favor.88 That is, the
plaintiff cannot just assert that a close relationship exists, but when the plaintiff
pleads specific facts about the relationship—such as the length of the relationship or

124 A.3d 1017, 1024 n.25 (Del. 2015)).
87 In re Oracle Corp. Derivative Litig., 824 A.2d 917, 938 (Del. Ch. 2003) (“Delaware law should
not be based on a reductionist view of human nature that simplifies human motivations on the lines
of the least sophisticated notions of the law and economics movement.”); see also Sanchez, 124
A.3d at 1022 (“Close friendships of that duration are likely considered precious by many people,
and are rare. People drift apart for many reasons, and when a close relationship endures for that
long, a pleading stage inference arises that it is important to the parties.”).
88 Sanchez, 124 A.3d at 1022 (“In that consideration, it cannot be ignored that although the plaintiff
is bound to plead particularized facts in pleading a derivative complaint, so too is the court bound
to draw all inferences from those particularized facts in favor of the plaintiff, not the defendant,
when dismissal of a derivative complaint is sought.”).
details about the closeness of the relationship—then this Court is charged with making all reasonable inferences from those facts in the plaintiff’s favor.\textsuperscript{89}

From the pled facts, there is reason to doubt Rankin’s capacity to impartially decide whether to sue members of the Kruse family. For starters, one can reasonably infer that Rankin’s successful career as a businessperson was in large measure due to the opportunities and mentoring given to him by Ed Kruse, Paul Kruse’s father, and other members of the Kruse family. The complaint alleges that Rankin started as Ed Kruse’s administrative assistant and, over the course of a 28-year career with the company, rose to the high managerial position of CFO.\textsuperscript{90} Not only that, but Rankin was added to Blue Bell’s board in 2004,\textsuperscript{91} which one can reasonably infer was due to the support of the Kruse family. Capping things off, the Kruse family spearheaded charitable efforts that led to a $450,000 donation to a key local college, resulting in Rankin being honored by having Blinn College’s new agricultural facility named after him.\textsuperscript{92} On a cold complaint, these facts support a reasonable inference that there are very warm and thick personal ties of respect, loyalty, and affection between Rankin and the Kruse family, which creates a reasonable doubt

\textsuperscript{89} Id. (holding that at the pleading stage this Court is “bound to draw all inferences from those particularized facts in favor of the plaintiff, not the defendant, when dismissal of a derivative complaint is sought”).
\textsuperscript{91} Id.
\textsuperscript{92} Id.
that Rankin could have impartially decided whether to sue Paul Kruse and his subordinate Bridges.

Even though Rankin had ties to the Kruse family that were similar to other directors that the Court of Chancery found were sufficient at the pleading stage to support an inference that they could not act impartially in deciding whether to cause Blue Bell to sue Paul Kruse,\textsuperscript{93} the Court of Chancery concluded that because Rankin had voted differently from Paul Kruse on a proposal to separate the CEO and Chairman position, these ties did not matter.\textsuperscript{94} In doing so, the Court of Chancery ignored that the decision whether to sue someone is materially different and more important than the decision whether to part company with that person on a vote about corporate governance, and our law’s precedent recognizes that the nature of the decision at issue must be considered in determining whether a director is independent.\textsuperscript{95} As important, at the pleading stage, the Court of Chancery was bound

\textsuperscript{93}Marchand v. Barnhill, 2018 WL 4657159, at *14–15 (Del. Ch. Sept. 27, 2018) (holding that two directors who both worked at Blue Bell for most, if not all, of their entire careers were beholden to the Kruse family and therefore not independent for demand futility).

\textsuperscript{94}Id. at *15.

\textsuperscript{95}See Sandys v. Pincus, 152 A.3d 124, 134 (Del. 2016) (“Causing a lawsuit to be brought against another person is no small matter, and is the sort of thing that might plausibly endanger a relationship.”); Sciabacucchi v. Liberty Broadband Corp., 2018 WL 3599997, at *14 (Del. Ch. July 26, 2018) (“It is reasonable to infer that, if Zinterhofer voted to authorize a derivative suit against Malone, the relationship between Searchlight and Liberty Global might be in jeopardy. After all, “[c]ausing a lawsuit to be brought against another person is no small matter, and is the sort of thing that might plausibly endanger a relationship.””); In re Oracle Corp. Derivative Litig., 824 A.2d 917, 940 (Del. Ch. 2003) (“In evaluating the independence of a special litigation committee, this court must take into account the extraordinary importance and difficulty of such a committee’s responsibility. It is, I daresay, easier to say no to a friend, relative, colleague, or boss
to accord the plaintiff the benefit of all reasonable inferences, and the pled facts fairly support the inference that Rankin owes an important debt of gratitude and friendship to the Kruse family for giving him his first job, nurturing his progress from an entry level position to a top manager and director, and honoring him by spearheading a campaign to name a building at an important community institution after him. Although the fact that fellow directors are social acquaintances who occasionally have dinner or go to common events does not, in itself, raise a fair inference of non-independence, our law has recognized that deep and long-standing friendships are meaningful to human beings and that any realistic consideration of the question of independence must give weight to these important relationships and their natural effect on the ability of the parties to act impartially toward each other. As in cases like *Sandys v. Pincus* and *Delaware County Employees Retirement Fund v. Sanchez*, the important personal and business

who seeks assent for an act (e.g., a transaction) that has not yet occurred than it would be to cause a corporation to sue that person. This is admittedly a determination of so-called ‘legislative fact,’ but one that can be rather safely made. Denying a fellow director the ability to proceed on a matter important to him may not be easy, but it must, as a general matter, be less difficult than finding that there is reason to believe that the fellow director has committed serious wrongdoing and that a derivative suit should proceed against him.” (footnotes omitted).

97 152 A.3d 124, 130 (Del. 2016) (holding that owning an airplane with the interested party “is suggestive of the type of very close personal relationship that, like family ties, one would expect to heavily influence a human’s ability to exercise impartial judgment”).
98 124 A.3d 1017, 1020–22 (Del. 2015) (holding that being “close personal friends for more than five decades” with the interested party gives rise to “a pleading stage inference . . . that it is important to the parties” and suggests that the director is not independent).
relationship that Rankin and the Kruse family have shared supports a pleading-stage inference that Rankin cannot act independently.

Because the complaint pleads particularized facts that raise a reasonable doubt as to Rankin’s independence, we reverse the Court of Chancery’s dismissal of the plaintiff’s claims against management for failure to adequately plead demand futility.

B. The Caremark Claim

The plaintiff also challenges the Court of Chancery’s dismissal of his Caremark claim. Although Caremark claims are difficult to plead and ultimately to prove out, we nonetheless disagree with the Court of Chancery’s decision to dismiss the plaintiff’s claim against the Blue Bell board.

Under Caremark and Stone v. Ritter, a director must make a good faith effort to oversee the company’s operations. Failing to make that good faith effort breaches the duty of loyalty and can expose a director to liability. In other words,

99 See Stone v. Ritter, 911 A.2d 362, 372 (Del. 2006) (“[A] claim that directors are subject to personal liability for employee failures is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.”) (internal quotation marks omitted); Guttman v. Huang, 823 A.2d 492, 506 (Del. Ch. 2003) (“A Caremark claim is a difficult one to prove.”); In re Caremark Int’l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996) (“The theory here advanced is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment.”).

100 Caremark, 698 A.2d at 970 (“It is important that the board 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 as a matter of ordinary operations, so that it may satisfy its responsibility.”).

29
for a plaintiff to prevail on a Caremark claim, the plaintiff must show that a fiduciary acted in bad faith—“the state of mind traditionally used to define the mindset of a disloyal director.”

Bad faith is established, under Caremark, when “the directors [completely] fail[] to implement any reporting or information system or controls[,] or . . . having implemented such a system or controls, consciously fail[] to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.” In short, to satisfy their duty of loyalty, directors must make a good faith effort to implement an oversight system and then monitor it.

As with any other disinterested business judgment, directors have great discretion to design context- and industry-specific approaches tailored to their companies’ businesses and resources. But Caremark does have a bottom-line requirement that is important: the board must make a good faith effort—i.e., try—to

---

101 Desimone v. Barrows, 924 A.2d 908, 935 (Del. Ch. 2007).
102 Stone, 911 A.2d at 370–72.
103 In re Citigroup Inc. S’holder Derivative Litig., 964 A.2d 106, 125–26 (Del. Ch. 2009) (Chandler, C.) (noting that Caremark “does not eviscerate the core protections of the business judgment rule”); Caremark, 698 A.2d at 970 (“Obviously the level of detail that is appropriate for such an information system is a question of business judgment.”); Desimone, 924 A.2d at 935 n.95 (noting that the approaches boards take to monitoring the corporation under their Caremark duty “will obviously vary because of the different circumstances corporations confront”); see also Caremark, 698 A.2d at 971 (“But, of course, the duty to act in good faith to be informed cannot be thought to require directors to possess detailed information about all aspects of the operation of the enterprise. Such a requirement would simple [sic] be inconsistent with the scale and scope of efficient organization size in this technological age.”).
put in place a reasonable board-level system of monitoring and reporting.\textsuperscript{104} Thus, our case law gives deference to boards and has dismissed Caremark cases even when illegal or harmful company activities escaped detection, when the plaintiffs have been unable to plead that the board failed to make the required good faith effort to put a reasonable compliance and reporting system in place.\textsuperscript{105}

For that reason, our focus here is on the key issue of whether the plaintiff has pled facts from which we can infer that Blue Bell’s board made no effort to put in place a board-level compliance system. That is, we are not examining the effectiveness of a board-level compliance and reporting system after the fact. Rather, we are focusing on whether the complaint pleads facts supporting a reasonable inference that the board did not undertake good faith efforts to put a board-level system of monitoring and reporting in place.

\textsuperscript{104} Stone, 911 A.2d at 370; see also Caremark, 698 A.2d at 971 (“Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation, . . . only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability.”).

\textsuperscript{105} See, e.g., Stone, 911 A.2d at 372–73 (dismissing a Caremark claim despite the fact that the company violated the Bank Secrecy Act and was fined $50 million); In re General Motors Derivative Litig., 2015 WL 3958724, at *1, 17 (Del. Ch. 2015) (dismissing a Caremark claim despite the fact that the company’s actions “led to monetary loss on the part of the corporation, via fines, damages and punitive damages from lawsuits; reputational damage; and most distressingly, personal injury and death to GM customers”); In re Citigroup Inc. S’holder Derivative Litig., 964 A.2d at 127 (dismissing a Caremark claim despite the fact that the company suffered billions of dollars in losses because of its exposure to subprime mortgages).
Under Caremark, a director may be held liable if she acts in bad faith in the sense that she made no good faith effort to ensure that the company had in place any “system of controls.”106 Here, the plaintiff did as our law encourages and sought out books and records about the extent of board-level compliance efforts at Blue Bell regarding what has to be one of the most central issues at the company: whether it is ensuring that the only product it makes—ice cream—is safe to eat.107 Using these books and records, the complaint fairly alleges that before the listeria outbreak engulfed the company:

- no board committee that addressed food safety existed;
- no regular process or protocols that required management to keep the board apprised of food safety compliance practices, risks, or reports existed;
- no schedule for the board to consider on a regular basis, such as quarterly or biannually, any key food safety risks existed;
- during a key period leading up to the deaths of three customers, management received reports that contained what could be considered red, or at least yellow, flags, and the board minutes of the relevant period revealed no evidence that these were disclosed to the board;

106 Stone, 911 A.2d at 370; see also Caremark, 698 A.2d at 971 (“Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation, . . . only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability.”).
107 Though, to be fair and completely accurate, Blue Bell does make a few other related products, such as frozen yogurt.
• the board was given certain favorable information about food safety by management, but was not given important reports that presented a much different picture; and

• the board meetings are devoid of any suggestion that there was any regular discussion of food safety issues.

And the complaint goes on to allege that after the *listeria* outbreak, the FDA discovered a number of systematic deficiencies in all of Blue Bell’s plants—such as plants being constructed “in such a manner as to [not] prevent drip and condensate from contaminating food, food-contact surfaces, and food-packing material”—that might have been rectified had any reasonable reporting system that required management to relay food safety information to the board on an ongoing basis been in place.\(^\text{108}\)

In sum, the complaint supports an inference that no system of board-level compliance monitoring and reporting existed at Blue Bell. Although *Caremark* is a tough standard for plaintiffs to meet, the plaintiff has met it here. When a plaintiff can plead an inference that a board has undertaken no efforts to make sure it is informed of a compliance issue intrinsically critical to the company’s business operation, then that supports an inference that the board has not made the good faith effort that *Caremark* requires.

\(^{108}\) App. to Opening Br. at A94–96 (Food and Drug Administration Inspection Report for Blue Bell Creameries facility in Sylacauga, Alabama (Apr. 30, 2015)).
In defending this case, the directors largely point out that by law Blue Bell had to meet FDA and state regulatory requirements for food safety, and that the company had in place certain manuals for employees regarding safety practices and commissioned audits from time to time.\footnote{Throughout the document, footnotes are used to cite specific sources or additional information.} In the same vein, the directors emphasize that the government regularly inspected Blue Bell’s facilities, and Blue Bell management got the results.\footnote{Answering Br. at 28–29; see also Marchand v. Barnhill, 2018 WL 4657159, at *17 (Del. Ch. Sept. 27, 2018) (“[D]ocuments incorporated by reference in the Complaint reveal that Blue Bell distributed a sanitation manual with standard operating and reporting procedures, and promulgated written procedures for processing and reporting consumer complaints. Blue Bell engaged a third-party laboratory and food safety auditor to test for the presence of dangerous contaminates in its facilities.”).}

But the fact that Blue Bell nominally complied with FDA regulations does not imply that the board implemented a system to monitor food safety \textit{at the board level}.\footnote{Stone, 911 A.2d at 368 (“To the contrary, the Caremark Court stated, ‘it is important that the \textit{board} exercise a good faith judgment that the corporation’s information and reporting system is in concept and design adequate to assure the \textit{board} that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.’”) (quoting Caremark, 698 A.2d at 970) (emphasis added).} Indeed, these types of routine regulatory requirements, although important, are not typically directed at the board. At best, Blue Bell’s compliance with these requirements shows only that management was following, in a nominal way, certain standard requirements of state and federal law. It does not rationally suggest that the board implemented a reporting system to monitor food safety or Blue Bell’s operational performance. The mundane reality that Blue Bell is in a highly regulated
industry and complied with some of the applicable regulations does not foreclose any pleading-stage inference that the directors’ lack of attentiveness rose to the level of bad faith indifference required to state a Caremark claim.

In answering the plaintiff’s argument, the Blue Bell directors also stress that management regularly reported to them on “operational issues.” This response is telling. In decisions dismissing Caremark claims, the plaintiffs usually lose because they must concede the existence of board-level systems of monitoring and oversight such as a relevant committee, a regular protocol requiring board-level reports about the relevant risks, or the board’s use of third-party monitors, auditors, or consultants.112 For example, in Stone v. Ritter, although the company paid $50

112 See, e.g., City of Birmingham Ret. Sys. v. Good, 177 A.3d 47, 59 (Del. 2017) (affirming the Court of Chancery’s dismissal of a Caremark claim because “reports to the board showed that the board ‘exercised oversight by relying on periodic reports’ from the officers” and that board presentations “identified issues with the coal ash disposal ponds, but also informed the board of the actions taken to address the regulatory concerns”); Stone, 911 A.2d at 372–73 (affirming the Court of Chancery’s dismissal of a Caremark claim, in part, because an outside auditor’s report “reflect[s] that the Board received and approved relevant policies and procedures, delegated to certain employees and departments the responsibility for filing [suspicious activity reports] and monitoring compliance, and exercised oversight by relying on periodic reports from them”); In re General Motors Derivative Litig., 2015 WL 3958721, at *14 (Del. Ch. 2015) (dismissing a Caremark claim where “GM had a system for reporting risk to the Board, but in the Plaintiffs’ view it should have been a better system”); In re Citigroup Inc. S’holder Derivative Litig., 964 A.2d 106, 127 (Del. Ch. 2009) (dismissing a Caremark claim because “[p]laintiffs do not contest that Citigroup had procedures and controls in place that were designed to monitor risk”); Desimone v. Barrows, 924 A.2d 908, 940 (Del. Ch. 2007) (dismissing a Caremark claim premised on the plaintiff’s allegations that a properly formed and well-functioning audit committee must have known about options backdating despite the fact that management intentionally kept this information from the audit committee); Guttmann v. Huang, 823 A.2d 492, 506–07 (Del. Ch. 2003) (dismissing a Caremark claim because the plaintiff failed to plead any particularized facts about the audit committee’s lack of reporting or information systems).
million in fines related “to the failure by bank employees” to comply with “the federal Bank Secrecy Act,”\footnote{911 A.2d at 365–66.} the “[b]oard dedicated considerable resources to the [Bank Secrecy Act] compliance program and put into place numerous procedures and systems to attempt to ensure compliance.”\footnote{Id. at 371.} Accordingly, this Court affirmed the Court of Chancery’s dismissal of a \textit{Caremark} claim. Here, the Blue Bell directors just argue that because Blue Bell management, in its discretion, discussed general operations with the board, a \textit{Caremark} claim is not stated.

But if that were the case, then \textit{Caremark} would be a chimera. At every board meeting of any company, it is likely that management will touch on some operational issue. Although \textit{Caremark} may not require as much as some commentators wish,\footnote{See, e.g., John Armour, et al., \textit{Board Compliance}, 104 MINNESOTA L. REV. (forthcoming 2020) (manuscript at 47), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205600; John Armour & Jeffrey N. Gordon, \textit{Systemic Harms and Shareholder Value}, 6 J. LEGAL ANALYSIS 35, 46 (2014); Hillary A. Sale, \textit{Monitoring Caremark’s Good Faith}, 32 DEL. J. CORP. L. 719, 753 (2007).} it does require that a board make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation’s central compliance risks. In Blue Bell’s case, food safety was essential and mission critical. The complaint pled facts supporting a fair inference that no board-level system of monitoring or reporting on food safety existed.
If Caremark means anything, it is that a corporate board must make a good faith effort to exercise its duty of care. A failure to make that effort constitutes a breach of the duty of loyalty. Where, as here, a plaintiff has followed our admonishment to seek out relevant books and records\textsuperscript{116} and then uses those books and records to plead facts supporting a fair inference that no reasonable compliance system and protocols were established as to the obviously most central consumer safety and legal compliance issue facing the company, that the board’s lack of efforts resulted in it not receiving official notices of food safety deficiencies for several years, and that, as a failure to take remedial action, the company exposed consumers to listeria-infected ice cream, resulting in the death and injury of company customers, the plaintiff has met his onerous pleading burden and is entitled to discovery to prove out his claim.

\textbf{III. Conclusion}

We therefore reverse the Court of Chancery’s decision and remand for proceedings consistent with this opinion.

\textsuperscript{116}\textit{See Sandys v. Pincus}, 152 A.3d 124, 128 (Del. 2016) (“For many years, this Court and the Court of Chancery have advised derivative plaintiffs to take seriously their obligations to plead particularized facts justifying demand excusal.”).
The United States Securities and Exchange Commission’s (“Commission”) Division of Enforcement (“Division”), in consultation with the Division of Corporation Finance and the Office of the Chief Accountant, investigated whether certain public issuers that were victims of cyber-related frauds may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls.

As discussed more fully below, the issuers—a group that spans numerous industries—each lost millions of dollars as a result of cyber-related frauds. In those frauds, company personnel received spoofed or otherwise compromised electronic communications purporting to be from a company executive or vendor, causing the personnel to wire large sums or pay invoices to accounts controlled by the perpetrators of the scheme. Spoofed or manipulated electronic communications are an increasingly familiar and pervasive problem, exposing individuals and companies, including public companies, particularly those that engage in transactions with foreign customers or suppliers, to significant risks and financial losses. The Federal Bureau of Investigation recently estimated that these so-called “business email compromises” had caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017—the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period.1

In connection with the investigation, the Commission considered whether the issuers complied with the requirements of Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934.

---

1 FBI, 2017 Internet Crime Report at 12, 21 (issued May 7, 2018) available at https://pdf.ic3.gov/2017_IC3Report.pdf (“FBI Internet Crime Report”) (the FBI defines business email compromise as “a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payments,” and includes frauds impacting both private and public companies); FBI, Public Service Announcement: E-Mail Account Compromise the 5 Billion Dollar Scam (May 4, 2017), available at https://www.ic3.gov/media/2017/170504.aspx (“FBI PSA”); see also Proofpoint, 2017 Email Fraud Threat Report at 3 (Feb. 12, 2018) available at https://www.proofpoint.com/sites/default/files/pfpt-us-tr-email-fraud-yir-180212.pdf (finding that by the fourth quarter of 2017, nearly 89% of all organizations were targeted by at least one attack, over a 13% increase from the fourth quarter of 2016).

Those provisions require certain issuers to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management’s general or specific authorization. As the Senate emphasized over four decades ago when passing these provisions, “[a] fundamental aspect of management’s stewardship responsibility is to provide shareholders with reasonable assurances that the business is adequately controlled.” While the cyber-related threats posed to issuers’ assets are relatively new, the expectation that issuers will have sufficient internal accounting controls and that those controls will be reviewed and updated as circumstances warrant is not.

The Commission has determined not to pursue an enforcement action in these matters based on the conduct and activities of these public issuers that are known to the Commission at this time. The Commission, however, deems it appropriate and in the public interest to issue this Report of Investigation (“Report”) pursuant to Section 21(a) of the Exchange Act to make issuers and other market participants aware that these cyber-related threats of spoofed or manipulated electronic communications exist and should be considered when devising and maintaining a system of internal accounting controls as required by the federal securities laws. Having sufficient internal accounting controls plays an important role in an issuer’s risk management approach to external cyber-related threats, and, ultimately, in the protection of investors.

II. INVESTIGATIONS

The Division’s investigation focused on the internal accounting controls of nine issuers that were victims of one of two variants of schemes involving spoofed or compromised electronic communications from persons purporting to be company executives or vendors. The issuers covered a range of sectors including technology, machinery, real estate, energy, financial, and consumer goods, reflecting the reality that every type of business is a potential target of

---


3 The issuers with these Section 13(b)(2) obligations are those that have a class of securities registered with the Commission under Section 12 of the Exchange Act or that must file reports with the Commission under Section 15(d) of the Exchange Act. 15 U.S.C. § 78m(b)(6). Also the level of reasonable assurances required under these provisions is defined as such “degree of assurance as would satisfy prudent officials in the conduct of their own affairs.” 15 U.S.C. § 78m(b)(7).

cyber-related fraud. At the time of the cyberscams, each issuer had substantial annual revenues and had securities listed on a national securities exchange.

Each of the nine issuers lost at least $1 million; two lost more than $30 million. In total, the nine issuers lost nearly $100 million to the perpetrators, almost all of which was never recovered. Some of the investigated issuers were victims of protracted schemes that were only uncovered as a result of third-party actions, such as through detection by a foreign bank or law enforcement agency. Indeed, one company made 14 wire payments requested by the fake executive over the course of several weeks—resulting in over $45 million in losses—before the fraud was uncovered by an alert from a foreign bank. Another of the issuers paid eight invoices totaling $1.5 million over several months in response to a vendor’s manipulated electronic documentation for a banking change; the fraud was only discovered when the real vendor complained about past due invoices.

Emails from Fake Executives. The first type of business email compromise the Division reviewed involved emails from persons not affiliated with the company purporting to be company executives. In these situations, the perpetrators of the scheme emailed company finance personnel, using spoofed email domains and addresses of an executive (typically the CEO) so that it appeared, at least superficially, as if the email were legitimate. In all of the frauds, the spoofed email directed the companies’ finance personnel to work with a purported outside attorney identified in the email, who then directed the companies’ finance personnel to cause large wire transfers to foreign bank accounts controlled by the perpetrators. The perpetrators used real law firm and attorney names, and legal services-sounding email domains like “consultant.com,” but the contact details connected company personnel with an impersonator and co-conspirator. These were not sophisticated frauds in general design or the use of technology. In fact, from a technological perspective they only required creating an email address to mimic the executive’s address. Each of the schemes had some common elements:

- The spoofed emails described time-sensitive transactions or “deals” that needed to be completed within days, and emphasized the need for secrecy from other company employees. They sometimes implied some level of government oversight, such as one fraudulent email claiming the purported transaction was “in coordination with and under the supervision of the SEC.”

- The spoofed emails stated that the funds requested were necessary for foreign transactions or acquisitions, and directed the wire transfers to foreign banks and beneficiaries. Although all of the issuers had some foreign operations, these purported foreign transactions would have been unusual for most of them. The emails also provided minimal details about the transactions.

---

• The spoofed emails typically were sent to midlevel personnel, who were not generally responsible or involved in the purported transactions (and who rarely communicated with the executives being spoofed). The emails also often included spelling and grammatical errors.

Emails from Fake Vendors. The second type of cyber-related fraud involved electronic communications impersonating the issuers’ vendors. This form of scam was more technologically sophisticated than the spoofed executive emails because, in the instances the Division reviewed, the schemes involved intrusions into the email accounts of issuers’ foreign vendors. After hacking the existing vendors’ email accounts, the perpetrators inserted illegitimate requests for payments (and payment processing details) into electronic communications for otherwise legitimate transaction requests. The perpetrators of these scams also corresponded with unwitting issuer personnel responsible for procuring goods from the vendors so that they could gain access to information about actual purchase orders and invoices. The perpetrators then requested that the issuer personnel initiate changes to the vendors’ banking information, and attached doctored invoices reflecting the new, fraudulent account information. The issuer personnel responsible for procurement relayed that information to accounting personnel responsible for maintaining vendor data. As a result, the issuers made payments on outstanding invoices to foreign accounts controlled by the impersonator rather than the accounts of the real vendors.

Unlike the fake executive scams, the spoofed vendor emails had fewer indicia of illegitimacy or red flags. In fact, several victims only learned of the scam when the real vendor raised concerns about nonpayment on outstanding invoices. Because vendors often afford issuers months before considering a payment delinquent, the scams, in certain circumstances, were able to continue for an extended period of time.

III. DISCUSSION

The Commission recently emphasized that “cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.” Accordingly, the Commission Statement and Guidance on Public Company Cybersecurity Disclosures advised such public companies that “[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws.”

---


7 Commission Statement on Cybersecurity Disclosures at 18.
In light of the risks associated with today’s ever expanding digital interconnectedness, public companies should pay particular attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds. More specifically, Section 13(b)(2)(B)(i) and (iii) require certain issuers to “devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management’s general or specific authorization,” and that “(iii) access to assets is permitted only in accordance with management’s general or specific authorization.”8 As the Senate underscored when these provisions were passed, “[t]he expected benefits from the conscientious discharge of these responsibilities are of basic importance to investors and the maintenance of the integrity of our capital market system.”9

Virtually all economic activities now take place through digital technology and electronic communication, leaving business transactions and assets susceptible to a variety of cyber-related threats.10 This is a growing global problem, and cyberscams like the ones described above that target an issuer’s assets are an ever-increasing part of the cybersecurity threats faced by a wide variety of businesses, including issuers with Section 13(b)(2)(B) obligations.11 The financial and other impacts of these frauds can be significant, as the instances described above attest.

As noted above, these frauds were not sophisticated in design or the use of technology; instead, they relied on technology to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective. Having internal accounting control systems that factor in such cyber-related threats, and related human vulnerabilities, may be vital to maintaining a sufficient accounting control environment and safeguarding assets.

These examples underscore the importance of devising and maintaining a system of internal accounting controls attuned to this kind of cyber-related fraud, as well as the critical role training plays in implementing controls that serve their purpose and protect assets in compliance with the federal securities laws. The issuers here, for instance, had procedures that required

9 1977 Senate Report at 8.
10 See, e.g., World Economic Forum Report at 14 (“Attacks are increasing, both in prevalence and disruptive potential.”).
11 See FBI Internet Crime Report at 12 (“In 2017, the IC3 received 15,690 BEC/EAC complaints with adjusted losses of over $675 million”); FBI PSA (“The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses.”). These figures include losses sustained by private or public companies, and so are not limited to those with securities registered under Section 12 of the Exchange Act or those that must file reports under Section 15(d) of the Exchange Act.
certain levels of authorization for payment requests, management approval for outgoing wires, and verification of any changes to vendor data. Yet they still became victims of these attacks. The existing controls could be (and were) interpreted by the company’s personnel to mean that the (ultimately compromised) electronic communications were, standing alone, sufficient to process significant wire transfers or changes to vendor banking data. To that end, after falling victim to these frauds, each of the issuers sought to enhance their payment authorization procedures, and verification requirements for vendor information changes. Moreover, as noted above, many of these issuers only learned of the fraud as a result of third-party notices, such as from law enforcement or foreign banks. Thereafter, these issuers took steps to bolster their account reconciliation procedures and outgoing payment notification processes to aid detection of payments resulting from fraud.\textsuperscript{12}

Systems of internal accounting controls, by their nature, depend also on the personnel that implement, maintain, and follow them. In the context of the business email compromises the Division reviewed, the frauds succeeded, at least in part, because the responsible personnel did not sufficiently understand the company’s existing controls or did not recognize indications in the emailed instructions that those communications lacked reliability. For example, in one matter, the accounting employee who received the spoofed email did not follow the company’s dual-authorization requirement for wire payments, directing unqualified subordinates to sign-off on the wires. In another, the accounting employee misinterpreted the company’s authorization matrix as giving him approval authority at a level reserved for the CFO. And there were numerous examples where the recipients of the fraudulent communications asked no questions about the nature of the supposed transactions, even where such transactions were clearly outside of the recipient employee’s domain and even where the employee was asked to make multiple payments over days and even weeks. In two instances the targeted recipients were themselves executive-level employees—chief accounting officers—who initiated payments in response to fake executive emails. To this end, while most of the issuers had some form of training regarding controls and information technology in place prior to the scams, all of them enhanced their training of responsible personnel about relevant threats, as well as about pertinent policies and procedures following the frauds.

IV. CONCLUSION

By this report, the Commission is not suggesting that every issuer that is the victim of a cyber-related scam is, by extension, in violation of the internal accounting controls requirements of the federal securities laws. What is clear, however, is that internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. Public issuers subject to the requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly.

Ultimately, issuers themselves are in the best position to develop internal accounting controls that account for their particular operational needs and risks in complying with Section 13(b)(2)(B). In performing this analysis, issuers should evaluate to what extent they should consider cyber-related threats when devising and maintaining their internal accounting control systems. Given the prevalence and continued expansion of these attacks, issuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks.

---

13 See 1977 Senate Report at 8 (“... management must exercise judgment in determining the steps to be taken, and the cost incurred, in giving assurance that the objectives expressed, will be achieved.”); Council of Economic Advisers Report at 45 (“Private firms are ultimately in the best position to figure out the most appropriate sector- and firm-specific cybersecurity practices.”).
SEcurities and exchange commission

17 CFR parts 229 and 249

[Release nos. 33-10459; 34-82746]

commission statement and guidance on public company cybersecurity disclosures

agency: Securities and Exchange Commission.

action: Interpretation.

summary: The Securities and Exchange Commission (the “Commission”) is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

Dates: Applicable: February 26, 2018

For further information contact: Questions about specific filings should be directed to staff members responsible for reviewing the documents the company files with the Commission. For general questions about this release, contact the Office of the Chief Counsel at (202) 551-3500 in the Division of Corporation Finance, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

Supplementary information:
I. Introduction
A. Cybersecurity

Cybersecurity risks pose grave threats to investors, our capital markets, and our country.¹

¹ The U.S. Computer Emergency Readiness Team defines cybersecurity as “[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.” U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#C (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May
Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks. Companies today rely on digital technology to conduct their business operations and engage with their customers, business partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.

As companies’ exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased.2 Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century. Cybersecurity incidents3 can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and “hacktivists.”4 Companies face an evolving

---


3 A “cybersecurity incident” is “[a]n occurrence that actually or potentially results in adverse consequences to … an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.” U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#I.

4 One study using a sample of 419 companies in 13 countries and regions noted that 47 percent of data breach incidents in 2016 involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures. See
landscape of cybersecurity threats in which hackers use a complex array of means to perpetrate cyber-attacks, including the use of stolen access credentials, malware, ransomware, phishing, structured query language injection attacks, and distributed denial-of-service attacks, among other means. The objectives of cyber-attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners. Cyber-attacks may also be directed at disrupting the operations of public companies or their business partners. This includes targeting companies that operate in industries responsible for critical infrastructure.

Companies that fall victim to successful cyber-attacks or experience other cybersecurity incidents may incur substantial costs\(^5\) and suffer other negative consequences, which may include:

- remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;\(^6\)
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;

---

\(^5\) The average organizational cost of a data breach in the United States in 2016 was $7.35 million based on the sample in the study. \textit{Id.} However, the total costs a company may incur in connection with a particular cyber-attack or incident could be much higher.

\(^6\) A company’s costs may also include payments to perpetrators of ransomware attacks in order to attempt to restore operations or protect customer data or other proprietary information. \textit{But see} Federal Bureau of Investigation, “How To Protect your Network from Ransomware,” Ransomware Prevention and Response for CISOs, available at https://www.justice.gov/criminal-ccips/file/872771/download.
• lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
• litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;\(^7\)
• increased insurance premiums;
• reputational damage that adversely affects customer or investor confidence; and
• damage to the company’s competitiveness, stock price, and long-term shareholder value.

Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack. Crucial to a public company’s ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.\(^8\) In addition, the Commission believes that the development of effective disclosure controls and procedures is best achieved when a company’s directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has

\(^7\) See, e.g., New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies; European Union General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 1.

\(^8\) See Section II.B.1 below for further discussion of disclosure controls and procedures.
faced or is likely to face.

Additionally, directors, officers, and other corporate insiders must not trade a public company’s securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company. Public companies should have policies and procedures in place to (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company’s discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information. In addition, we believe that companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material. We recognize that many companies have adopted preventative measures to address the appearance of improper trading and we encourage companies to consider such preventative measures in the context of a cyber event.

B. CF Disclosure Guidance: Topic No. 2

In October 2011, the Division of Corporation Finance (the “Division”) issued guidance that provided the Division’s views regarding disclosure obligations relating to cybersecurity risks and incidents. The guidance explains that, although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be

---

9 See Section II.B.2 below for further discussion of insider trading.

}

C. Purpose of Release

In light of the increasing significance of cybersecurity incidents, the Commission believes it is necessary to provide further Commission guidance. This interpretive release outlines the Commission’s views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies.\footnote{This release does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations. For example, in 2014 the Commission adopted Regulation Systems Compliance and Integrity, applicable to certain self-regulatory organizations, to strengthen the technology infrastructure of the U.S. securities markets. Final Rule: Regulation Systems Compliance and Integrity, Release No. 34-73639 (Nov. 19, 2014) [79 FR. 72252 (Dec. 5, 2014)], available at https://www.sec.gov/rules/final/2014/34-73639.pdf. For additional cybersecurity regulations and resources, see the Commission’s website page devoted to cybersecurity issues, available at https://www.sec.gov/spotlight/cybersecurity; see also Cybersecurity Guidance; IM Guidance Update (April 2015), available at https://www.sec.gov/investment/im-guidance-2015-02.pdf (staff guidance on cybersecurity measures for registered investment companies and investment advisers).} While the Commission continues to consider other means of promoting appropriate disclosure of cyber incidents, we are reinforcing and expanding upon the staff’s 2011 guidance. In addition, we address two topics not developed in the staff’s 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make
accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws.

Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.\(^\text{14}\)

The Commission, and the staff through its filing review process, continues to monitor cybersecurity disclosures carefully.

### II. Commission Guidance

#### A. Overview of Rules Requiring Disclosure of Cybersecurity Issues

1. **Disclosure Obligations Generally; Materiality**

Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act of 1933 (“Securities Act”) and the Securities Exchange Act of 1934 (“Exchange Act”), and periodic and current reports under the Exchange Act.\(^\text{15}\) When a company is required to file a disclosure


\(^{15}\) Listed companies also should consider any obligations that may be imposed by exchange listing requirements. For example, the NYSE requires listed companies to “release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities.” See NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments. In addition, in 2015, the NYSE, in partnership with Palo Alto Networks, published a summary of information about legal and regulatory aspects of cybersecurity governance for directors and officers of public companies. See Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc., 2015, available at https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf. Similarly, Nasdaq requires listed companies to “make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors’ decisions.” See Nasdaq Listing Rule 5250(b)(1).
document with the Commission, the requisite form generally refers to the disclosure requirements of Regulation S-K\textsuperscript{16} and Regulation S-X.\textsuperscript{17} Although these disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to disclose such risks and incidents depending on a company’s particular circumstances. For example:

- **Periodic Reports:** Companies are required to file periodic reports\textsuperscript{18} to disclose specified information on a regular and ongoing basis.\textsuperscript{19} These periodic reports include annual reports on Form 10-K,\textsuperscript{20} which require companies to make disclosure regarding their business and operations, risk factors, legal proceedings, management’s discussion and analysis of financial condition and results of operations (“MD&A”), financial statements, disclosure controls and procedures, and corporate governance.\textsuperscript{21} Periodic reports also include quarterly reports on Form 10-Q,\textsuperscript{22} which require companies to make disclosure regarding their

\begin{itemize}
    \item [16] 17 CFR part 229.
    \item [18] An issuer with a class of securities registered under Section 12 or subject to Section 15(d) of the Exchange Act is subject to the periodic and current reporting requirements of Section 13 and 15(d), respectively, of the Exchange Act.
    \item [19] “Congress recognized that the ongoing dissemination of accurate information by companies about themselves and their securities is essential to effective operation of the trading markets. The Exchange Act rules require public companies to make periodic disclosures at annual and quarterly intervals, with other important information reported on a more current basis. The Exchange Act specifically provides for current disclosure to maintain the currency and adequacy of information disclosed by companies.” Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, Release No. 33-8106, 3-4 (Jun. 17, 2002) [67 FR 42914 (Jun. 25, 2002)].
    \item [20] 17 CFR 249.310.
    \item [21] See Part I, Items 1, 1A and 3 of Form 10-K; Part II, Items 7, 8 and 9A of Form 10-K; and Part III, Item 10 of Form 10-K [17 CFR 249.310].
    \item [22] 17 CFR 249.308a.
\end{itemize}
financial statements, MD&A, and updated risk factors.\textsuperscript{23} Likewise, foreign private issuers are required to make many of these same disclosures in their periodic reports on Form 20-F.\textsuperscript{24} Companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.

- **Securities Act and Exchange Act Obligations:** Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.\textsuperscript{25}

- **Current Reports:** In order to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents,\textsuperscript{26} companies can provide current reports on Form 8-K\textsuperscript{27} or Form 6-K.\textsuperscript{28} Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity

\textsuperscript{23} See Part I, Items 1 and 2 of Form 10-Q; Part II, Item 1A of Form 10-Q [17 CFR 249.308a].

\textsuperscript{24} See Part I, Items 3.D, 4, 5 and 8 of Form 20-F; Part II, Items 15 and 16G of Form 20-F; Part III, Items 17 and 18 of Form 20-F [17 CFR 249.220f].


\textsuperscript{26} See Item 11(a) of Form S-3 [17 CFR 239.13] and Item 5(a) of Form F-3 [17 CFR 239.33].

\textsuperscript{27} 17 CFR 249.308.

\textsuperscript{28} 17 CFR 249.306.
incidents.\textsuperscript{29} The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur.\textsuperscript{30}

In addition to the information expressly required by Commission regulation, a company is required to disclose “such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading.”\textsuperscript{31} The Commission considers omitted information to be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available.\textsuperscript{32}

In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact

\textsuperscript{29}“The registrant may, at its option, disclose under this Item 8.01 [of Form 8-K] any events, with respect to which information is not otherwise called for by this form, that the registrant deems of importance to security holders.” 17 CFR 308.

\textsuperscript{30} See Sections II.B.2 and II.B.3 below for further discussion of insider trading and Regulation FD.


\textsuperscript{32} This approach is consistent with the standard of materiality articulated by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (a fact is material “if there is a substantial likelihood that a reasonable shareholder would consider it important” in making an investment decision or if it “would have been viewed by the reasonable investor as having significantly altered the ‘total mix’ of information made available” to the shareholder).
of the incident on the company’s operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations.\textsuperscript{33} The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause.\textsuperscript{34} This includes harm to a company’s reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts – for example, by providing a “roadmap” for those who seek to penetrate a company’s security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale

\textsuperscript{33} For example, the compromised information might include personally identifiable information, trade secrets or other confidential business information, the materiality of which may depend on the nature of the company’s business, as well as the scope of the compromised information.

\textsuperscript{34} As part of a materiality analysis, a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity. Basic v. Levinson, 485 U.S. 224, 238 (1988) (citing SEC v. Texas Gulf Sulphur Co., 401 F. 2d 833, 849 (2d Cir. 1968)). Moreover, no “single fact or occurrence” is determinative as to materiality, which requires an inherently fact-specific inquiry. Basic, 485 U.S. at 236.
of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.  

Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

We remind companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made (for example, when the original statement is still being relied on by reasonable investors). Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

35 See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15 U.S.C. 78o(d); 17 CFR 240.10b-5].

36 See Backman v. Polaroid Corp., 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies “if a disclosure is in fact misleading when made, and the speaker thereafter learns of this.”).

37 See id. at 17 (describing the duty to update as potentially applying “if a disclosure ‘becomes materially misleading in light of subsequent events’” (quoting Greenfield v. Heublein, Inc., 742 F.2d 751, 758 (3d Cir. 1984))). But see Higginbotham v. Baxter Intern., Inc., 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); Gallagher v. Abbott Laboratories, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).
We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we “emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies.”

Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

2. Risk Factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company’s securities speculative or risky. Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.

It would be helpful for companies to consider the following issues, among others, in evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;


39 17 CFR 229.503(c); 17 CFR 249.220f.

• the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company’s ability to prevent or mitigate certain cybersecurity risks;

• the aspects of the company’s business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks;

• the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;

• the potential for reputational harm;

• existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and

• litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose
particular risks to the company’s business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

3. **MD&A of Financial Condition and Results of Operations**

   Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations.\(^41\) In this context, the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company’s analysis. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation,

\(^41\) 17 CFR 229.303; 17 CFR 249.220f.
and the loss of competitive advantage that may result.\textsuperscript{42} Finally, the Commission expects companies to consider the impact of such incidents on each of their reportable segments.\textsuperscript{43}

4. **Description of Business**

Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions.\textsuperscript{44} If cybersecurity incidents or risks materially affect a company’s products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure.

5. **Legal Proceedings**

Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party.\textsuperscript{45} Companies should note that this requirement includes any such proceedings that relate to cybersecurity issues. For example, if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.


\textsuperscript{43} 17 CFR 229.303(a).

\textsuperscript{44} 17 CFR 229.101; 17 CFR 249.220f.

\textsuperscript{45} 17 CFR 229.103.
6. **Financial Statement Disclosures**

Cybersecurity incidents and the risks that result therefrom may affect a company’s financial statements. For example, cybersecurity incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
- loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases; and
- diminished future cash flows, impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

The Commission expects that a company’s financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.46

7. **Board Risk Oversight**

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors’ role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board’s leadership structure.47 The Commission has previously said that “disclosure about the board’s involvement in the oversight of the risk management process should provide important information to

---


47 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.
investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company.”

A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company’s business, we believe this discussion should include the nature of the board’s role in overseeing the management of that risk.

In addition, we believe disclosures regarding a company’s cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

B. Policies and Procedures

1. Disclosure Controls and Procedures

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and

---


49 See Item 407(h) of Regulation S-K [17 CFR 229.407(h)].
other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.  

Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness. These rules define “disclosure controls and procedures” as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) “recorded, processed, summarized and reported, within the time periods specified in the Commission’s rules and forms,” and (2) “accumulated and communicated to the company’s management … as appropriate to allow timely decisions regarding required disclosure.”

A company’s disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company’s businesses. Information also must be

---

50 See Final Rule: Certification of Disclosure in Companies’ Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm (“We believe that, to assist principal executive and financial officers in the discharge of their responsibilities in making the required certifications, as well as to discharge their responsibilities in providing accurate and complete information to security holders, it is necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner.”); see also Section 10(b) of the Exchange Act and Rule 10b-5 thereunder [15 U.S.C. 78j(b); 17 CFR 240.10b-5].


52 Id.

53 See Final Rule: Certification of Disclosure in Companies’ Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm (“We believe that the new rules will help to ensure that an issuer’s systems grow and evolve with its business and are capable of producing Exchange Act reports that are timely, accurate and reliable.”).
evaluated in the context of the disclosure requirement of Exchange Act Rule 12b-20.\textsuperscript{54} When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company’s business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

Exchange Act Rules 13a-14 and 15d-14\textsuperscript{55} require a company’s principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures,\textsuperscript{56} and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures.\textsuperscript{57} These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company’s ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

\textsuperscript{54} 17 CFR 240.12b-20.

\textsuperscript{55} 17 CFR 240.13a-14; 17 CFR 240.15d-14.

\textsuperscript{56} Section 302 of the Sarbanes-Oxley Act of 2002 required the Commission to adopt final rules under which the principal executive officer or officers and the principal financial officer or officers, or persons providing similar functions, of an issuer each must certify the information contained in the issuer’s quarterly and annual reports. Pub. L. 107-204, 116 Stat. 745 (2002).

\textsuperscript{57} 17 CFR 229.307; 17 CFR 249.220f.
2. **Insider Trading**

Companies and their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches.\(^{58}\) It is illegal to trade a security “on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information.”\(^{59}\) As noted above, information about a company’s cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company’s securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.\(^{60}\)

Beyond the antifraud provisions of the federal securities laws, companies and their directors, officers, and other corporate insiders must comply with all other applicable insider trading related rules. Many exchanges require listed companies to adopt codes of conduct and policies that promote compliance with applicable laws, rules, and regulations, including those prohibiting insider trading.\(^{61}\) We encourage companies to consider how their codes of ethics\(^{62}\)

---

\(^{58}\) In addition to promoting full and fair disclosure, the antifraud provisions of the federal securities laws prohibit insider trading, which harms not only individual investors but also the very foundations of our markets by undermining investor confidence in the integrity of those markets. 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

\(^{59}\) Rule 10b5-1(a) of the Exchange Act [17 CFR 240.10b-5-1(a)].

\(^{60}\) This would not preclude directors, officers, and other corporate insiders from relying on Exchange Act Rule 10b5-1 if all conditions of that rule are met.

\(^{61}\) See *e.g.*, NYSE Listed Company Manual Section 303A.10, which states in relevant part that every NYSE “listed company should proactively promote compliance with laws, rules and regulations, including insider trading laws.
and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. The Commission believes that it is important to have well designed policies and procedures to prevent trading on the basis of all types of material non-public information, including information relating to cybersecurity risks and incidents.

In addition, while companies are investigating and assessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents, they should consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. Company insider trading policies and procedures that include prophylactic measures can protect against directors, officers, and other corporate insiders trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident. As noted above, we believe that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.

3. Regulation FD and Selective Disclosure

Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Under Regulation FD, “when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information.” The Commission adopted Regulation FD owing to concerns

Insider trading is both unethical and illegal, and should be dealt with decisively.” See also NASDAQ Listing Rule 5610 and Section 406(c) of the Sarbanes-Oxley Act of 2002.


about companies making selective disclosure of material nonpublic information to certain persons before making full disclosure of that same information to the general public.  

In cases of selective disclosure of material nonpublic information related to cybersecurity, companies should ensure compliance with Regulation FD. Companies and persons acting on their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing that same information to the public. We expect companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to

\[\text{Footnotes}\]

\[\text{Footnotes continued}\]

\[\text{Footnotes ended}\]
cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made simultaneously (in the case of an intentional disclosure as defined in the rule) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation.67

By the Commission.

Dated: February 21, 2018

Brent J. Fields
Secretary

---

67 “Under the regulation, the required public disclosure may be made by filing or furnishing a Form 8-K, or by another method or combination of methods that is reasonably designed to effect broad, non-exclusionary distribution of the information to the public.” Id. at 3.
BIOGRAPHY OF KEVIN A. ZERRUSEN

Kevin Zerrusen is the Senior Advisor to the SEC Chairman for Cybersecurity Policy. Prior to joining the SEC, he worked as a Managing Director at Goldman Sachs, where he led initiatives to strengthen technology risk governance, incident management and insider threat programs. He previously served as Chair of the Intelligence National Security Alliance’s Cyber Council, a group chartered to promote effective public-private sector collaboration on cybersecurity issues, and is a veteran of the Central Intelligence Agency, where his duties included running the agency’s cyber center, which was responsible for analyzing, evaluating, and countering foreign cyber threats. Mr. Zerrusen has an M.B.A. from Syracuse University and a Bachelor’s degree from the University of Dayton.
William R. Denny
Partner

William R. Denny has a business and litigation practice, focusing on commercial and corporate transactions, vendor management, mergers and acquisitions, data privacy and security and information technology. Mr. Denny is a Certified Information Privacy Professional (CIPP/US) and a Certified Information Privacy Manager (CIPM) through the International Association of Privacy Professionals (IAPP). He has represented public and privately held companies and government entities in a wide range of technology transactions, including negotiating complex cloud services agreements, software and IT infrastructure development, maintenance and support agreements, long-term materials supply agreements, outsourcing agreements, transition and site services agreements, technology licensing agreements, sales of internet domain names, and website terms of use and privacy policies. Clients include major corporations in the industrial, chemical, medical and technology sectors, as well as technology and information systems service providers and developers.

Mr. Denny has litigated disputes over the interpretation and enforcement of many types of technology contracts, general commercial contracts and liability insurance policies. He has tried jury and non-jury cases in federal and state trial and appellate courts, before arbitration panels, and by use of other alternative dispute resolution techniques.

Mr. Denny took a leading role in drafting and negotiating Delaware’s amendment to its computer security breach law, 6 Del. C. §§ 12B-100 et seq., which was enacted in June 2017 and came into force in April 2018.

Mr. Denny writes extensively on technology and business issues, including:

- “Standing and the Circuit Court Split in Data Breach Litigation” in Corporate Disputes, January-March 2018
- “Representations and Warranties in M&A Agreements” in the ABA’s Guide to Cybersecurity Due Diligence in M&A Transactions, December 2017
America 2017 in the area of Information Technology Law.
AV® rated by Martindale-Hubbell.
Delaware State Bar Association; Co-Chair, E-Discovery and Technology Law Section; Committee on Professional Ethics (former Co-Chair)
American Bar Association; Business Section, Cyberspace Law Committee; Co-Chair, IT Services and Cloud Computing Subcommittee; Cybersecurity Legal Task Force
Federal Bar Association, Ad Hoc Committee for Electronic Discovery
Richard K. Herrmann Technology American Inn of Court

● "What's Changed Under Delaware's New Data Breach Law" in Law360, August 24, 2017
● "Building Your Cyber Incident Response Plan" in Delaware Business, May/June 2017
● "Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act" in Business Law Today, June 2016

Mr. Denny frequently speaks at seminars, programs and meetings on topics including technology, e-discovery and cybersecurity, among others:

● March 29, 2019, at the ABA Section of Business Law Spring Meeting in Vancouver, BC, Canada, Mr. Denny presented: “Cross-border Cybersecurity Compliance Issues.”
● November 14, 2018, at a program sponsored by the Delaware State Bar Association on Cybersecurity Recent Developments, Mr. Denny presented on the California Consumer Privacy Act and the move toward new federal legislation in privacy.
● October 31, 2018, at the Secure Delaware 2018 Workshop, organized by the State of Delaware's Department of Technology and Innovation, Mr. Denny presented “Data Privacy and the Double Trouble of the GDPR and the California Consumer Privacy Act of 2018”.
● September 14, 2018, at the ABA Business Section Annual Meeting in Chicago, IL, Mr. Denny moderated a program entitled “Blockchain Basics for the Business Lawyer – Smart Contracts, Crypto Offerings and Other Transformative Applications.”
● August 2, 2018, at the ABA Annual Meeting in Chicago, IL, Mr. Denny presented “Cybersecurity Law: Deciphering the Landscape of Legal Requirements Applicable To Businesses and Law Firms.”
● May 31, 2018, at the Business Law Basics Webinar sponsored by the American Bar Association, Mr. Denny presented on Data Privacy.
● May 2, 2018, at a program sponsored by the Delaware Bioscience Association, Mr. Denny presented on Data Security for IP.
● April 12, 2018, at the ABA Section of Business Law Spring Meeting in Orlando, FL, Mr. Denny moderated and presented on a program panel entitled, “Best Practices for Compliance Programs to Mitigate Risks of Cyber Incidents.”
● January 25, 2018, at a Delaware State Bar Association program, Mr. Denny presented Cybersecurity Recent Developments.