May 9, 2022

Vanessa A. Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File No. S7-09-22, RIN 3235-AM89); 87 Fed. Reg. 16,590 (Mar. 23, 2022)

Dear Ms. Countryman:

Better Markets[1] appreciates the opportunity to comment on the above-captioned Proposed Rule ("Proposal" or "Release")[2] intended to enhance disclosure of cybersecurity risks, governance, and incidents in our financial markets. The Proposal has two primary components. First, it would require publicly traded companies to disclose their policies and procedures that identify and manage ***cybersecurity risks***; management's role in governing those risks; any expertise of the board of directors in cybersecurity and its oversight of cybersecurity risks; and updated disclosures of previously reported cybersecurity incidents in its Form 10-K. Second, the Proposal would require publicly traded companies to disclose ***cybersecurity incidents*** to investors in Form 8-K within four days after determining it has experienced a material cybersecurity incident.

The Proposal builds off previous guidance issued by the staff and the Commission to ensure more standardized and timely disclosures to investors of cybersecurity risks, governance, and incidents. The proposed Item 106 disclosures in Form 10-K will better inform investors of the cybersecurity risks posed to the operations, reputation, and financials of a publicly traded company. Additionally, the proposed Item 1.05 in Form 8-K will inform investors of material cybersecurity incidents promptly, which will minimize the ability of corporate insiders and malicious actors to trade on material, nonpublic information at the expense of investors. The

[1] Better Markets is a non-profit, non-partisan, and independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support the financial reform of Wall Street, and make our financial system work for all Americans again. Better Markets works with allies—including many in finance—to promote pro-market, pro-business, and pro-growth policies that help build a stronger, safer financial system that protects and promotes Americans' jobs, savings, retirements, and more.

[2] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16,590 (Mar. 23, 2022).

1825 K Street, NW, Suite 1080, Washington, DC 20006 TELEPHONE (1) 202.618-6464 FAX (1) 202.618.6465 WEBSITE bettermarkets.com

Commission should move forward with the Proposal after adding the enhancements described below.

BACKGROUND

Speaking on the topic of cybersecurity in 2012, former Federal Bureau of Investigation Director Robert Mueller said "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[3] The former FBI Director's words are just as true now, if not more so, than they were back in 2012. While technology has revolutionized the way corporations conduct business, it has not come without its own set of risks and vulnerabilities. A 2019 survey of cybersecurity professionals reinforces the former FBI Director's statement, with almost half of respondents reporting an increase of cyberattacks on their organization and 79 percent reporting they expect to experience a cyberattack next year.[4] The question of whether or not a company will experience a cyberattack is becoming less a matter of "if" it will happen and more of a matter of "when" it will happen and how much damage will it cause.

The rise in the sheer number of cyberattacks and their growing sophistication has led many to acknowledge cybersecurity threats as one of the top risks facing the private sector. In the World Economic Forum's Global Risks Perception Survey, respondents cited cyberattacks and data fraud or theft as two of the top five global risks. This is in stark contrast with the results from the same survey conducted ten years earlier, which mentioned neither cyberattacks nor data fraud among the top five global risks.[5] To help put the perceived risks surrounding cybersecurity into context with other risks posed to companies, the PricewaterhouseCoopers' Annual Global CEO Survey found that cybersecurity edged out the COVID-19 global health crisis as the threat CEOs are most worried about over the next 12 months.[6] That point bears repeating—CEOs view the potential threat of a cyberattack or data breach to be a greater threat to their company than the risk posed by a global pandemic, a pandemic that has unfolded over two years and exacted a huge toll in human life and economic suffering.

Just as we have seen the economic damage a global pandemic can have on companies of all sizes, we have also seen the crippling effects a major cyberattack or data breach can have on a company. For example, we saw the largest gas pipeline operator and largest meat processing plant in the U.S. forced to halt operations due to a pair of cyberattacks in 2021 that cut off 45% of the oil to the East Coast and halted production of a company that provides one-fifth of the U.S.'s meat

---

3 Robert S. Mueller, Director, FBI, RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

4 Press Release, Information Systems Audit and Control Association, New Study Reveals Cybercrime May Be Widely Underreported – Even When Laws Mandate Disclosure (June 3, 2019), New Study Reveals Cybercrime May Be Widely Underreported Even When Laws Mandate Disclosure (isaca.org).

5 World Economic Forum, The Global Risks Report 8 (2019), https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

6 PricewaterhouseCoopers, *Reimagining the outcomes that matter* (Jan. 17, 2022), https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html.

supply.[7] In addition, malware and ransomware attacks increased in 2020 by 358% and 435%, respectively, from the previous year.[8] When you combine the debilitating consequences of a successful cyberattack, combined with the relentless threat of attack, it is no wonder cybersecurity is the top threat to U.S. companies cited by CEOs. Unfortunately, this trend shows little sign of abating in the near future as businesses become more dependent on digitizing their operations and storing more and more valuable data within their networking systems. This all serves as further motivation and riper targets for cybercriminals to ramp up their cyberattacks.

For each data breach, experts have estimated that the average cost per record breached was $161 in 2021, a 14.2% increase since 2017.[9] While $161 per record may not seem like a large sum of money in isolation, it actually suggests huge collective costs, as cybercriminals are less likely to target individuals and more likely to target businesses and organizations with vast troves of data representing thousands and millions of records. This number also does not account for the financial damage wreaked on the individual consumer or investor who has had their sensitive information breached, which can be debilitating and devastating. In the case of large breaches, the financial damage of a cyberattack or data breach can have consequential and systemic consequences not only in the markets but also on society as a whole.

A few large breaches have become case studies on how not to handle a significant cyberattack. In 2014, the company formerly known as Yahoo! Inc., learned that hackers had stolen the usernames, email addresses, phone numbers, birthdates, and passwords for hundreds of millions of user accounts.[10] Although senior management and the legal department at Yahoo! Inc. were well aware of the breach, the company did not disclose the breach to its investors or the public until two years after the attack, in a filing during the process of being acquired by Verizon Communications, Inc.[11] The Commission ordered Yahoo! Inc. to pay a $35 million penalty.[12] Moreover, Verizon subsequently cut the price it was willing to pay for Yahoo! Inc. by $350 million after news of the data breach was announced.[13] After the close of the sale, it was discovered that all three billion Yahoo! Inc. user accounts were affected by the hack. This episode vividly illustrated how not to handle a cyberattack and data breach after one has occurred; just as important, it also showed that a company's failure to have policies and procedures in place to deal effectively with a cyberattack can affect vast numbers of investors. In this case, aside from users having their private information hacked, Yahoo! Inc. investors lost more than $500 million in fines, shareholder lawsuit costs, and a lower sale price due to these failures by the company.

Another example of a corporate cybersecurity failure is the Equifax cyberattack and data breach. In 2017, hackers successfully gained access to Equifax's database of information on 143

---

7 *See* Financial Stability Oversight Council, Annual Report 62 (2021).

8 World Economic Forum, The Global Risks Report 9 (2019), https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

9 IBM, Cost of a Data Breach Report 13 (2021), https://www.ibm.com/downloads/cas/OJDVQGRY.

10 Altaba Inc., No. 3-18448 2 (Securities Exchange Commission April 24, 2018).

11 *Id.*

12 *Id.* at 9.

13 Vindu Goel, *Verizon Will Pay $350 Million Less for Yahoo*, N.Y. Times, Feb. 17, 2017, https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html?_r=0.

million American consumers, including social security numbers, driver's license numbers, and more than 200,000 credit card numbers.[14] Hackers were able to penetrate Equifax's systems after Equifax failed to update a critical patch to address a vulnerability in its network. Executives at the company were made aware of the loss of personal identifiable information on July 31, but they did not disclose the breach to the public until September 7 via a press release.[15] For five weeks, Equifax insiders withheld knowledge of this breach of sensitive, personal identifiable information from shareholders, investors, policymakers, and the public at large. This cybersecurity failure was further compounded when certain high-ranking employees were able to sell their stock in the company during the five-week period before the breach was announced to the public.[16] After the announcement of the data breach, Equifax's stock price plummeted 35%, and those employees pocketed hundreds of thousands of dollars in savings from selling their stock before disclosure. Equifax later agreed to a settlement of nearly $1 billion with regulators[17] and agreed to spend an additional $1 billion on cybersecurity upgrades.[18]

Both major incidents occurred in spite of the Commission's staff guidance regarding disclosure obligations for cybersecurity risks and cyber incidents issued in 2011. This staff guidance was the Commission's first foray into cybersecurity risk and incident disclosure. At the time, and to this day, the securities laws and rules contained no disclosure requirements specifically relating to cybersecurity risks and incidents.[19] However, as the risks posed by cyber threats to publicly traded companies continued to mount, the Commission took the view that those risks and incidents could trigger the longstanding obligation to disclose material information to investors.[20] For the first time, the staff guidance laid out an overview of how cybersecurity risks and cyber incidents may fall under various types of disclosure obligations, including disclosure as part of a company's risk factors; management's discussion and analysis of financial condition and results of operations; description of business; financial statement disclosures prior to, during, and after a cyber incident; and disclosure controls and procedures.[21]

As a result of the increasing significance of cybersecurity incidents and in the wake of the Yahoo! Inc. and Equifax data breaches, the Commission believed it necessary to provide further guidance in connection with cybersecurity disclosure requirements under the federal securities laws in 2018.[22] The 2018 Commission guidance reinforced and expanded upon the 2011 guidance with two additional topics, including "the importance of cybersecurity policies and procedures and

---

14 *Examining the Equifax Data Breach: Hearing Before the H. Committee on Financial Services*, 115th Cong. (2017) (statement of Richard F. Smith, Chairman and Chief Executive Officer, Equifax).

15 *Id.*

16 *See* Press Release, SEC, *Former Equifax Manager Charged With Insider Trading*, https://www.sec.gov/news/press-release/2018-115.

17 *FTC v. Equifax, Inc.*, No. 1:19-cv-03297-TWT (N.D. Ga. July 23, 2019).

18 *Equifax, Inc.* Customer Data Breach Litigation, No. 1:17-md-2800-TWT (N.D. Ga. Jan. 13, 2020).

19 SEC, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011).

20 *Id.*

21 *Id.*

22 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018).

the application of insider trading prohibitions in the cybersecurity context."[23] The new guidance document built upon the 2011 staff guidance, but it stressed the importance of creating and maintaining policies and procedures related to cybersecurity to ensure accurate and timely disclosure of material events, and it reminded companies that cybersecurity risks and incidents could rise to the level of material, nonpublic information for which insider trading prohibitions applied.[24]

The COVID-19 pandemic and the changes to the modern workplace that have come as a result of the pandemic have only elevated the risk of cyberattacks. The increase in remote work has made companies and organizations more vulnerable to cyberattacks through the increased use of teleworking strategies, including virtual meeting applications and virtual private networks.[25] Research has found that data breaches where remote work was a factor in the breach increased the total cost of a breach by $1.07 million on average.[26] This raises the level of vigilance that all companies must maintain in connection with cybersecurity vulnerabilities and further demonstrates the growing risk cybersecurity poses to corporate America.

OVERVIEW OF THE PROPOSAL

The Commission has proposed several rule amendments governing disclosure of cybersecurity risk management policies, procedures, and incidents by registrants. Specifically, the Proposal would:

- Amend Form 8-K to require registrants to disclose material information about a cybersecurity ***incident within four business days*** after the registrant determines a material cybersecurity incident has occurred;

- Amend Forms 10-Q and 10-K to require registrants to provide regular ***updated disclosures relating to previously disclosed cybersecurity incidents***, as well as require registrants to amend these forms when individually immaterial cybersecurity incidents have become material in the aggregate;

- Amend Form 10-K to require registrants to ***disclose their policies and procedures*** for identifying and managing cybersecurity risks; ***management's role and expertise*** in assessing and managing cybersecurity risks and implementing policies and procedures; and the ***expertise, if any, of the board of directors*** and its oversight role of cybersecurity risk;

- Amend Regulation S-K to require disclosure of any cybersecurity ***expertise by any member of the board of directors***;

---

23 *Id.* at 8,167.
24 *Id.*
25 Financial Stability Oversight Council, Annual Report 62 (2021).
26 IBM, Cost of a Data Breach Report 13 (2021), https://www.ibm.com/downloads/cas/OJDVQGRY.

- Amend Form 20-F to require ***foreign private issuers*** to disclose cybersecurity policies, procedures, and incidents similar to domestic registrants;

- Amend Form 6-K to add ***"cybersecurity incidents"*** as a reporting topic; and

- Require the cybersecurity disclosures to be presented in ***Inline eXtensible Business Reporting Language*** (Inline XBRL).

COMMENTS

I. Mandatory and uniform cybersecurity disclosure requirements in proposed Item 106 will better inform investors about the cybersecurity risks posed to companies.

The Proposal's cybersecurity risk, governance, and incident disclosure requirements in Item 106 of Regulation S-K will better inform investors of the cybersecurity risks posed to the operations, reputation, and financials of a publicly traded company. While existing securities laws, regulations, and case law currently require registrants to report material information, there are no disclosure requirements that specifically refer to cybersecurity risks or incidents other than the 2011 staff guidance and 2018 guidance adopted by the Commission. Despite the serious risk posed by cybersecurity to a business's operations, reputation, and financials, investors are often left to search for piecemeal disclosures regarding cybersecurity risks, policies and procedures, and incidents that management may elect to make in various places in a company's annual and quarterly reports. The Proposal's mandatory and uniform cybersecurity disclosure requirements in proposed Item 106 will better inform investors of the cybersecurity risks posed to companies and make it easier to find the relevant information.

As mentioned previously, cybersecurity is often cited by business leaders as the top risk or threat posed to their business. In fact, an analysis of Form 10-K filings of the Fortune 100 companies found that 100 percent of the companies listed cybersecurity as a risk factor in the risk factor disclosure section of their annual report.[27] Typically, a company would develop a set of risk management systems to deal with such a pervasive threat, one that executives and companies are acknowledging to investors.[28] These policies and procedures would normally be designed to identify, assess, and manage these risks, and they may be subject to oversight by the board and management.[29] However, staff in the Division of Corporation Finance have found that of those companies reporting cyber incidents in 2021, many of those same companies did not describe their oversight efforts or policies and procedures related to cybersecurity.[30] Notwithstanding the consensus surrounding the risk posed by cybersecurity in corporate America, there is a clear lack

---

27 Steve W. Klemash, Jamie C. Smith, and Chuck Seets, *What Companies are Disclosing About Cybersecurity Risk and Oversight*, Harvard Law School Forum on Corporate Governance (Aug. 25, 2020), https://corpgov.law.harvard.edu/2020/08/25/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight/.

28 Release at 16,599.

29 Release at 16,599.

30 Release at 16,599.

of uniformity surrounding how cybersecurity threatens specific business operations and the policies and procedures companies establish to mitigate those risks. While the disclosure of a cyber incident is helpful for investors to understand the risks posed to a company's business operations and financials, how a company responds to mitigate those risks may be just as important. Therefore, a company's cybersecurity policies and procedures disclosures are critical if investors are to truly understand the gravity of the incident and its possible effects on a company's bottom line and stock price. Accordingly, understanding a company's policies and procedures regarding cyberattacks is clearly necessary to assess the company's ability to prevent and blunt the impact of any *future* attacks.

One need look no further than the filing of Form 10-K for Pilgrim Pride Corporation as an example of this phenomenon. In 2021, the largest meat processing plant in the U.S. and the parent of the Pilgrim Pride Corporation, JBS USA Holdings Inc., suffered a crippling cyberattack that led to a halt in nearly all of its business operations, including those of the Pilgrim Pride Corporation.[31] After paying an $11 million ransom to the hackers, JBS USA Holdings was able to regain control of its systems and continue with regular business operations. Despite the company losing control of its business operations for an entire day, the disclosures in Pilgrim Pride Corporation's Form 10-K devoted only two paragraphs of a 118-page document to the event and other cybersecurity disclosures, all of which were buried under the heading "Business and Operation Risk Factors."[32] Despite losing control over its business operations, Pilgrim Pride Corporation determined that "none of these actual or attempted cyber-attacks has had a material effect on our operations or financial condition."[33] The 10-K filing continues with a very broad description of the event, without any mention of the company's cybersecurity policies and procedures. This demonstrates that even when a company suffers a severe cyber incident, they do not always, and in fact rarely, disclose corresponding cybersecurity policies and procedures to give investors any ability to evaluate the likelihood of future attacks and the ability of the company to mitigate and remediate their impact.

Even in instances where a company discloses relevant cybersecurity incidents, board and management oversights and abilities, and policies and procedures in a comprehensive manner, the information is scattered throughout various sections of the Form 10-K. While the 2018 guidance adopted by the Commission successfully identified potential disclosure requirements for companies to think about when disclosing cybersecurity risks, governance, and incidents, it did not solve the problem confronting investors who must search various sections of the Form 10-K for the disclosures. As the Proposal points out, these cybersecurity disclosures may currently be disclosed in:

- Item 105 of Regulation S-K (Risk Factors);

---

31 Fabiana Batista, Michael Hirtzer, and Mike Dorning, *All of JBS's U.S. Beef Plants Were Forced Shut by Cyberattack*, Bloomberg (May 31, 2021), https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs.

32 Pilgrim's Pride Corporation, Annual Report (Form 10-K) 11 (Feb. 18, 2022).

33 *Id.*

- Item 303 of Regulation S-K (Management's Discussion and Analysis of Financial Condition and Results of Operations);
- Item 101 of Regulation S-K (Description of Business);
- Item 103 of Regulation S-K (Legal Proceedings);
- Item 407 of Regulation S-K (Corporate Governance); and
- Regulation S-X Financial Disclosures.[34]

The scattered and unpredictable nature of such cybersecurity disclosures, which investors must search to locate in the Form 10-K, diminishes their effectiveness. It would be far more useful for investors to better understand the cybersecurity risks posed to specific companies if these disclosures were more uniform and easier to find, as laid out in the Proposal.

The proposed new Item 106 to Regulation S-K in the Proposal would provide investors with a more uniform and comprehensive understanding of the cybersecurity risks, governance, and incidents of publicly traded companies. Proposed Item 106 would require disclosure of updates to previously disclosed cybersecurity incidents, as well as:

- A registrant's policies and procedures, if any, for identifying and managing cybersecurity risks;
- A registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks; and
- Management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies.[35]

This will not only enable investors to better understand the cybersecurity risks, governance, and incidents of companies they are currently invested in but also enables them to more easily compare cybersecurity policies and procedures across different publicly traded companies when making investment decisions. As the top risk facing companies, according to the nation's CEOs, investors need this information in a readily accessible and readable fashion. In short, the proposed Item 106 to Regulation S-K would help investors gain a much better understanding of the always important and potentially catastrophic cybersecurity risks facing publicly traded companies.

The Proposal should be further strengthened to explicitly require registrants to disclose whether or not it has established any cybersecurity policies or procedures. Under the current requirements of the Proposal, a registrant would not have to explicitly state it has not established

[34] Release at 16,593-16,594.
[35] Release at 16,595.

cybersecurity policies and procedures if it has not done so. The Proposal rightfully asks the question, *should a registrant have to explicitly state that it has not established any cybersecurity policies and procedures*?[36] For many of the same reasons we support proposed Item 106, we would answer that question in the affirmative. As mentioned several times throughout this comment letter, cybersecurity is often considered to be the top risk facing companies. Therefore, it is appropriate for companies to disclose to investors if they have established policies and procedures to address this risk. Investors will surely want to know if there are policies and procedures in place at the companies they invest in to mitigate the risks of cyberattacks and data breaches, which can bring with them operational, reputational, and financial harm. Enabling companies that have not established cybersecurity policies and procedures to hide this fact from investors would undermine the intended goals of this Proposal to "better inform investors about a registrant's risk management, strategy, and governance."[37] For these reasons, the Proposal should require companies that have not established policies and procedures to inform investors of this critically important and potentially pivotal lapse in corporate governance.

The Proposal should also be strengthened by requiring a simple disclosure to investors of whether or not a registrant's cybersecurity risk assessment program has been audited by a third party. The Proposal partly addresses this concern in proposed Item 106(b), which would among other things, require disclosure of whether the "registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program."[38] The Proposal would provide more meaningful insight to investors about the resiliency of a company's cybersecurity risk assessment program if it required a simple disclosure as to whether the company's program was audited by a third party with expertise in auditing cybersecurity risk assessment programs annually. While a company may already have a comprehensive cybersecurity risk assessment program, the ever-changing landscape of cyberattacks makes it necessary to remain vigilant against these attacks, and periodic auditing helps maintain that vigilance. The auditing and testing of a company's cybersecurity risk assessment program by a third party that did not design or establish the program provides an extra check against cyberattacks by malicious actors. The audited status of a cybersecurity program would therefore provide investors with additional information with which they could assess a company's approach to managing cyber risk. Yet according to analysis of the annual reports of a representative group of 100 companies, only 17% of companies indicated that their policies and procedures were audited by a third party.[39] A clear disclosure in the Form 10-K would better inform investors about the cybersecurity risks posed to a company's business operations, reputation, and financials.

---

36 Release at 16,601.
37 Release at 16,590.
38 Release at 16,600.
39 Vaishnavi Ravishankar, Olivia Mooney, and Nore Hader, *Stepping Up Governance on Cyber Security*, Principles for Responsible Investment 5 (2018), https://www.unpri.org/download?ac=5134.

II. The Proposal's incident reporting requirement will inform investors of material cybersecurity attacks and data breaches in a timely manner and minimize the opportunity for corporate insiders and malicious actors to benefit financially.

The Proposal's cybersecurity incident reporting requirement will enable investors to learn about the operational, reputational, and financial risks to a company from a cyberattack in a timely and standardized manner. Despite past guidance issued by the Commission, the current cybersecurity incident reporting system is a hodgepodge of disclosures in Form 8-K, press releases, or periodic reports, including instances when a cybersecurity incident is reported through a press release but not reported in any filings with the Commission.[40] The Proposal would help ensure appropriate disclosures are made, in a standard form, and in a centralized location.

The Proposal's requirement that companies file Item 1.05 of Form 8-K within four days after experiencing a material cybersecurity incident will empower investors with important, timely, and standardized information regarding the operational, reputational, and financial risks to a company of a cyberattack or data breach. Additionally, Item 1.05 of Form 8-K will provide companies with a clear, standardized way of relaying this material information to investors, without having to wrestle with decisions about how to disclose a cyber incident. Thus, as cybersecurity risks continue to pose a top risk to companies, the Proposal's Item 1.05 of Form 8-K will help protect investors in a way that is fair and efficient from the standpoint of issuers.

The Proposal's four-day disclosure requirement will have the added benefit of minimizing the period of time corporate insiders and malicious actors will have to trade on material, nonpublic information before that information is disclosed to the public. As mentioned previously, the Equifax data breach was a case study in policy and procedure failures in responding to a cyberattack and data breach. More than five weeks passed from the time the company learned of the data breach and its disclosure to the public via a press release. During this five-week period, multiple corporate insiders sold large amounts of their stock in Equifax, pocketing hundreds of thousands of dollars prior to the public disclosure of the massive cyberattack.[41] Additionally, the four-day disclosure requirement would minimize the time during which hackers can profit from their own attacks in the markets. Hackers often target companies in search of a ransom payment or the opportunity to sell stolen data on the dark web, but they also have been known to sell information about their impending cyberattack to other bad actors or short a stock themselves to receive an additional financial benefit from their schemes.[42] The Proposal's four-day disclosure

---

40 Release at 16,594.

41 *See* Press Release, Department of Justice, Former Equifax manager sentenced for insider trading (Oct. 16, 2018), https://www.justice.gov/usao-ndga/pr/former-equifax-manager-sentenced-insider-trading.; Press Release, Department of Justice, Former Equifax employee sentenced for insider trading (June 27, 2019), https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading.

42 *See* Bradley Barth, *Ransomware gang offers traders inside scoop on attack victims so they can short sell their stocks* (Apr. 23, 2021), *https://www.scmagazine.com/news/security-news/ransomware/ransomware-gang-offers-traders-inside-scoop-on-attack-victims-so-they-can-short-sell-their-stocks* ("An entry on the DarkSide Leaks site dated April 20 states: 'Now our team and partners encrypt many companies that are trading on NASDAQ and other stock exchanges. If the company refuses to pay, we are ready to provide

requirement will substantially reduce the amount of time corporate insiders and malicious actors have to trade on inside information at the expense of investors.

The Proposal should further be strengthened by expanding the class of cyber incidents that trigger the reporting obligation. The Proposal currently includes a non-exhaustive list of examples of cybersecurity incidents that may trigger the four-day disclosure requirement, including "an incident in which a malicious actor has demanded payment to restore company *data that was stolen or altered*."[43] This example should be expanded to account for evolving kinds of cyberattacks that do not steal or alter company data but nevertheless generate illicit profits from the attack and have significant and adverse impacts on a business. As we saw in the Pilgrim Pride Corporation case, ransomware attacks can cripple a company's ability to conduct business without stealing or altering data. A ransomware attack has the ability to lock companies out of their own systems until a ransom is paid, as was the case with Pilgrim Pride Corporation. Thus, for example, the Proposal should provide that any cyberattack that ultimately extracts any form of payment from a company should be considered an example of a cybersecurity incident that would trigger the proposed Item 1.05 disclosure.

The need to broadly define the reportable incidents is clear. Despite the cyberattack shutting down operations at one of the largest meat-packing companies in the world, Pilgrim Pride Corporation's mention of the attack in its 10-K filing made it clear they did not believe this met the standard for a material event.[44] If all companies were to view cyberattacks through the same lens used by the Pilgrim Pride Corporation, then even attacks that have the ability to shut down business operations would be viewed as non-material events for which full disclosure was unnecessary. If allowed to prevail, this view would undermine the purposes of the Proposal. Therefore, the Proposal should take as broad a view as possible to ensure that any ransom or other payment related to a cyberattack requires disclosure.

CONCLUSION

We hope these comments are helpful as the Commission finalizes the Proposal.

Sincerely,

Stephen W. Hall
Legal Director and Securities Specialist

---

information before the publication, so that it would be possible to earn in the reduction price of shares. Write to us in 'Contact Us' and we will provide you with detailed information").

43 Release at 16,596.

44 Pilgrim's Pride Corporation, Annual Report (Form 10-K) 11 (Feb. 18, 2022).

Scott Farnin
Legal Counsel

Better Markets, Inc.
1825 K Street, NW
Suite 1080
Washington, DC 20006
(202) 618-6464

shall@bettermarkets.org
sfarnin@bettermarkets.org

http://www.bettermarkets.org