VERIZON COMMUNICATIONS INC
Form PX14A6G
April 03, 2018

April 2, 2018

Dear Verizon Communications Shareholders,

We are writing to urge Verizon Communications shareholders to VOTE FOR ITEM 7 on Verizon's 2018 proxy.

As data privacy protections and cyber security become increasingly important – witness Equifax, Facebook, and quickly escalating pressure from government and plaintiffs – we believe Verizon needs to demonstrate that it is doing everything it can to address this issue and address the catastrophically large Yahoo breach that it inherited. We believe that in this environment, the least the company can do is to explore how to maximize its executives' incentives on data privacy and cyber security through the company's compensation plans.

Trillium's shareholder proposal states:

Resolved: Verizon shareholders request the appropriate board committee(s) publish a report (at reasonable expense, within a reasonable time, and omitting confidential or propriety information) assessing the feasibility of integrating cyber security and data privacy metrics into the performance measures of senior executives under the company's compensation incentive plans.

As described more fully below:

- It is in the company's interest to explore how it can fully incentivize its executives to prevent data privacy and cyber security incidents.
- The pressure from consumers, government, and plaintiffs is only growing stronger – now is the time to demonstrate renewed efforts to protect data privacy and cyber security.
- Despite Verizon's protestations, it is fully capable of developing methods for linking executive compensation to data privacy and cyber security.

For the reasons provided below, we urge Verizon Communications shareholders to vote FOR ITEM 7 on the company proxy.

<u>While the company has management systems and oversight mechanisms in place, we believe it is prudent to explore additional mechanisms.</u>

It is unlikely that we know the full scope of the number and severity of Verizon's cyber security and data privacy incidents; however, we do know that the company has significant and persistent data privacy and cyber security controversies. Whether it is the warrantless wiretapping controversies post-9/11 or the 2016 Verizon Enterprise breach of 1.5 million customers,[1] we can see ongoing reasons for concern. There is the example from July 2017, when the Washington Post reported that a "communication breakdown and a vacationing employee were the reasons it took more than a week to close a leak [in June] that contained data belonging to 6 million Verizon customers"[2]. And of course, in October 2017, it was announced that all 3 billion accounts in subsidiary Yahoo had been breached prior to its acquisition by Verizon. This aspect of the Yahoo deal could have financial impacts for years to come.

There is no denying that Verizon has adopted management systems and oversight mechanisms to address these issues. But as we see at companies like Equifax, Facebook, Target, and many others, even cyber security plans which sound robust can in reality be insufficient. Even the "best" plans can be improved.

And the stakes are incredibly high. In September 2017, the Co-Director of the SEC's Enforcement Division announced the creation of a "Cyber Unit" stating, "Cyber-related threats and misconduct are among the greatest risks facing investors and the securities industry.[3] Prior to becoming the Chairman of the SEC, Jay Clayton wrote that "cyber-threats are among the most urgent risk to America's economic and national security and the personal safety of its citizens.[4] So it stands to reason that Verizon should at least give some serious consideration to assessing the feasibility of integrating cyber security and data privacy metrics into the performance measures of senior executives under the company's compensation incentive plans.

It should be pointed out that linking compensation to specific performance goals like this is not just a notional idea born out of whimsy. Rather, it is an idea from a United Kingdom Parliamentary committee study on cyber security which recommended "To ensure this issue receives sufficient CEO attention before a crisis strikes, a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the Board.[5]

We also know from at least one award winning scholarly work that this kind of linkage has been shown to be effective. Boston University Professor Caroline Flammer found in her recent study that:

---

[1] http://fortune.com/2016/03/24/verizon-enterprise-data-breach/
[2] https://www.washingtonpost.com/news/the-switch/wp/2017/07/17/why-it-took-more-than-a-week-to-resolve-the-verizon-data
[3] https://www.sec.gov/news/press-release/2017-176
[4] http://knowledge.wharton.upenn.edu/article/how-the-ten-commandments-of-cyber-security-can-enhance-safety/
[5] https://www.cio.com/article/3096966/security/cybersecurity-a-view-from-the-top.html

the adoption of CSR contracting leads to i) an increase in long-term orientation; ii) an increase in firm value; iii) an increase in social and environmental performance; iv) a reduction in emissions; and v) an increase in green innovations. These findings are consistent with our theoretical arguments predicting that CSR contracting helps direct management's attention to stakeholders that are less salient but financially material to the firm in the long run, thereby enhancing corporate governance.[6]

In light of this work done by both policy makers and academics, there is a compelling basis to conclude that Verizon should assess the feasibility of integrating cyber security and data privacy metrics into the performance measures of senior executives under the company's compensation incentive plans.

Verizon needs to do more in the face of growing expectations regarding cyber security and data privacy matters.

The unprecedented attention being paid to Facebook's latest data privacy and cyber security crisis strongly suggests that it is in Verizon's interest to do more to ensure that it is getting ahead of the issue. The revelations in the New York Times that the data of 50 million Facebook users had ended up in the wrong hands at Cambridge Analytica to be used for improper purposes has resulted in withering scrutiny from Federal policy makers and regulators, Congress, State Attorneys General, investors, civil society organizations, and consumers. Verizon could be only one mistake away from having a similar situation on its hands.

But one does not even need to look at other consumer facing companies to grow concerned. On March 2, 2018 there was a settlement of the Yahoo shareholder class action lawsuit for $80 million related to the 2016 data breaches. As widely respected management liability attorney, Kevin LaCroix pointed out – this litigation could be a breakthrough for the plaintiff's bar and could unleash even more litigation and higher damages.

---

[6] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2831694

The Yahoo settlement (assuming it is approved by the court) is the first significant data breach-related shareholder lawsuit settlement. The plaintiffs' lawyers have now figured at least one way they can make money off of this type of litigation. Interestingly, this settlement coincidentally comes just days after the SEC released new guidance in which the agency underscored the disclosure obligations of reporting companies that have experienced data breaches. It is hard to know for sure, but it could be this milestone settlement together with the SEC's new disclosure guidelines could mean that data breach-related shareholder litigation could be an area of increased focus for the plaintiffs' lawyers.[7]

The litigation risks for companies like Verizon are only growing, as are the expectations that the company is looking for the best ways to ensure they are managing and overseeing cyber security and data privacy protections.

The proposal is not overly burdensome to implement and provides the company the appropriate flexibility to implement.

The proposal simply asks "the appropriate board committee(s) publish a report (at reasonable expense, within a reasonable time, and omitting confidential or propriety information) assessing the feasibility of integrating cyber security and data privacy metrics into the performance measures of senior executives under the company's compensation incentive plans." As the proposal makes clear, it is providing the company full discretion to simply assess the feasibility of adopting these kinds of incentives. The proposal does not dictate any particular outcome or timeline. It does not seek to prescribe how a compensation plan would be constructed or how much weight cyber security and data privacy would have in the plan.

In addition, the assessment will not be burdensome. We recommend the company do the assessment at reasonable expense. In addition, the company has already conducted an assessment of the feasibility of integrating factors such as diversity, carbon emissions, and many financial metrics into compensation plans. Therefore, this is not a unique or difficult process for the company to embark upon.

Verizon's arguments in its statement of opposition are insufficient – it has already demonstrated the capability of implementing the proposal.

Verizon makes two direct arguments against the use of compensation linkages to address cyber security and data privacy: (1) it is difficult to link executive actions on cyber security and data privacy to outcomes and (2) there is no accepted methodology for measuring outcomes. These two arguments strike us as exceptionally weak. Verizon has ample capacity to conduct an assessment of the feasibility of integrating cyber security and data privacy metrics into the performance measures of senior executives under the company's compensation incentive plans. At a reasonable cost and with a reasonable allocation of resources, there is no doubt that Verizon's Board has the capability, analytical resources, and data to do an assessment.

[7] https://www.dandodiary.com/2018/03/articles/securities-litigation/yahoo-settles-data-breach-related-securities-suit-80-millior

Verizon seems to be arguing that it is only appropriate to link a performance metric to compensation when the executives "decisions have a direct impact on their achievement of the performance target" and not when there are external factors that may have an impact on the achievement of the target. However, Verizon currently links executive compensation to metrics such as earnings per share, free cash flow and revenue – all metrics that are not wholly dependent on executive decisions and are not entire free of external influence. Earnings, cash flow, and revenue are all subject to actions by consumers, regulators, competitors, and other factors that are far beyond the reach and influence of company executives. Nevertheless, Verizon has found an acceptable way to link compensation to these factors and shareholders have voted in favor of such compensation plans for many years.

With respect to Verizon's second argument, methodology, this argument is equally unpersuasive. Why can the company not define "success" as a very low number of breaches? Or zero breaches impacting more than a set number of individuals? Or perhaps success could be defined by a set of respected protocols such as the National Institute of Standards and Technology Cybersecurity Framework[8] or third party data privacy standards?[9]

However, we know from experience that Verizon already knows how to put a price and a value to the management of these risks. Last year Verizon renegotiated its acquisition of Yahoo after disclosure of the massive hacking incidents referred to earlier. Verizon's general counsel said in December[10] that the company felt it had "enough clarity that we can put parameters around the risk here and negotiate a deal that effectively compensates us for the risk." Verizon should now put a price on the performance of its own executives in addressing cyber security and data privacy concerns.

---

[8] https://www.nist.gov/cyberframework
[9] https://rankingdigitalrights.org
[10] https://www.wsj.com/articles/companies-sharpen-cyber-due-diligence-as-m-a-activity-revs-up-1520226061

Conclusion.

As described above, Trillium Asset Management is urging Verizon shareholders to support Item 7 on Verizon's proxy. We believe it is in the company's interest to explore how it can fully incentivize its executives to prevent data privacy and cyber security incidents. As the pressure from consumers, government, and plaintiffs is only growing stronger, now is the time to demonstrate renewed efforts to protect data privacy and cyber security. Finally, despite Verizon's protestations, it is fully capable of developing methods for linking executive compensation to data privacy and cyber security.

Sincerely,

Jonas Kron
Senior Vice President

IMPORTANT NOTICE: The cost of this communication is being borne entirely by Trillium Asset Management, LLC ("Trillium"). The foregoing information may be disseminated to shareholders via telephone, U.S. mail, e-mail, certain websites and certain social media venues, and should not be construed as investment advice or as a solicitation of authority to vote your proxy. The cost of disseminating the foregoing information to shareholders is being borne entirely by Trillium. Proxy cards will not be accepted by Trillium. To vote your proxy, please follow the instructions on your proxy card. These written materials may be submitted pursuant to Rule 14a-6(g)(1) promulgated under the Securities Exchange Act of 1934. Submission is not required of this filer under the terms of the Rule, but is made voluntarily in the interest of public disclosure and consideration of these important issues. The views expressed are those of the authors and Trillium as of the date referenced and are subject to change at any time based on market or other conditions. These views are not intended to be a forecast of future events or a guarantee of future results. These views may not be relied upon as investment advice. The information provided in this material should not be considered a recommendation to buy or sell any of the securities mentioned. It should not be assumed that investments in such securities have been or will be profitable. To the extent specific securities are mentioned, they have been selected by the authors on an objective basis to illustrate views expressed in the commentary and do not represent all of the securities purchased, sold or recommended for advisory clients. The information contained herein has been prepared from sources believed reliable but is not guaranteed by us as to its timeliness or accuracy, and is not a complete summary or statement of all available data. This piece is for informational purposes and should not be construed as a research report.