EQUIFAX INC
Form PX14A6G
April 11, 2018

April 11, 2018

Please vote on May 3, 2018, AGAINST the re-election of directors John McKinley, Mark B. Templeton and Mark L. Feidler at the annual meeting of Equifax Inc. (NYSE: EFX).

Dear Equifax shareholder,

Ahead of Equifax's annual shareholder meeting, we urge you to consider the extensive failures of risk oversight and internal control monitoring leading up to Equifax's 2017 data breach. While the company has taken certain remedial actions to correct its inadequate cybersecurity processes, we believe that in light of the size and scope of the data breach, greater board level accountability is required.

Taken as whole, the company's actions in the last several months have amounted to a reactive attempt to remedy a considerable defect in the company's cybersecurity and compliance practices, one that could have been avoided had the Board provided the requisite amount of oversight. The impact of the data breach on the company's performance is clear, with the stock dropping 16% since the breach was disclosed, compared to 6.4% for the S&P 500. As a consequence, shareholders must clearly signal that the Board's failure to provide adequate oversight over a critical component of the company's business operations has left shareholders with little option but to vote AGAINST directors McKinley, Templeton, and Feidler's reelection to the Board due to their long-term membership on the Technology Committee and failure to discharge their duties. In addition to his service on the Technology Committee, Mr. McKinley also serves as a long-term member of the Audit Committee. We believe a vote AGAINST these directors is warranted for the following reasons:

- **Failure to Act on Repeated Warnings and Known Risks:** Director McKinley, as a member of the Audit Committee and Chairman of the Technology Committee, and directors Templeton and Feidler, as members of the Technology Committee, failed to provide timely and adequate risk oversight over a material enterprise risk despite numerous warnings, which ultimately culminated in loss of over 147 million Americans' personal information.

- **Poor Crisis Management:** Director McKinley, as a member of the Audit Committee and Chairman of the Technology Committee, and directors Templeton and Feidler, as members of the Technology Committee, failed to develop a comprehensive crisis management plan in the wake of the breach, which further damaged the company's reputation as a leading provider that helps consumers protect their personal information and a premier credit monitoring agency.

- **Weak Supervision of the Company's Compliance Obligations:** Director McKinley, as a member of the Audit Committee, failed to provide adequate risk oversight of the company's legal and compliance obligations, particularly with regards to its insider trading policies.

The aforementioned nominees, as incumbent directors and tenured members of the Audit Committee and the Technology Committee at the time of the breach,[1] are the most responsible for failed response to the data breach that has led to significant scrutiny by federal regulators and other stakeholders. The company is currently being investigated by the Securities & Exchange Commission ("SEC"), Department of Justice, Federal Trade Commission, and congressional committees in both the House and Senate. It is now the subject of hundreds of lawsuits, four shareholder derivative suits, as well as civil investigative demands by 49 Attorneys General. With the estimated costs of the breach at approximately $275 million for just 2018 alone, experts have suggested that it could be the largest and most costly data breach in corporate history.

1 We note that Mr. Feidler now serves on the Compensation and Governance Committees. He was a member of the Technology Committee at the time that the data breach took place and when the announcement of the breach was made. He also previously served on the Technology Committee for several years prior to the breach.

The CtW Investment Group works with pension funds sponsored by unions affiliated with Change to Win, a federation of unions representing nearly 5.5 million members, to enhance long term shareholder value through active ownership. These funds invest over $250 billion in the global capital markets and are substantial investors of Equifax. We previously raised our concerns with the Board's oversight of risk management in October 2017 and in an in-person meeting in February 2018.

The Audit and Technology Committees Failed to Heed Multiple Warning Signs and Provided Poor Risk Oversight

The data breach announced in September 2017 exposed the company's weaknesses related to internal controls and risk oversight of the company's cybersecurity processes. From mid-May until July 29, 2017, criminals were able to exploit Equifax's weak cybersecurity processes to steal hundreds of millions of Americans' personal information over the course of approximately 10 weeks. The breach was based on a known vulnerability brought to the company's attention by the Department of Homeland Security and for which a patch had been available for two months prior to the hack even taking place.

Further warning signs of the inadequacy of the company's cybersecurity processes were evidenced by the fact that Mandiant, the same company hired by Equifax to investigate the breach, identified an additional and previously undisclosed March 2017 attack likely by the same hackers that conducted the May breach. In fact, index provider MSCI had warned Equifax almost a year before the breach was disclosed that Equifax was not equipped to respond to a data breach, finding no evidence that the company conducted regular cybersecurity audits or that it had adequate response plans in place. MSCI also removed the company from its index related to environmental, social and governance factors.

As a member of the Audit Committee, director McKinley was responsible for an annual review of risk assessment and risk management…including compliance and litigation risks facing the company.[2] Further, McKinley, with directors Templeton and Feidler, also sat on the Technology Committee, specifically charged with "identifying threats occasioned by new technologies, especially disruptive technologies" as well as reviewing the company's "technology investments and infrastructure related to risk management, including policies relating to information security.[3] In many ways, both the Audit Committee and the Technology Committee were empowered with the tools necessary to identify and possibly even avoid the massive data breach that took place, but failed to execute the responsibilities and duties required of them.

The Company's Inadequate Response Plans Amplified the Reputational Damage to the Company

Equifax's sluggish response to the cyber security breach is well documented. Former CEO and Chair Richard Smith waited three weeks before discussing with the full Board the details of the cybersecurity incident, and disclosed the breach to shareholders and the public almost six weeks after the discovery. Subsequent to the disclosure of the hack, the company found itself embroiled in a reputational crisis that was exacerbated by its own remediation attempts. From directing consumers to phishing sites, to requiring potential victims to submit partial social security number to Equifax to determine if their personal information was stolen, the series of missteps taken by the company after the breach implies that Equifax had done little in terms of crisis management planning. The financial impact of these missteps are

apparent. The company has lost over $2.5 billion in market cap since Q2 2017, a profitable IRS contract, and suffered cancellations by notable clients such as *The New York Times*.

2 Equifax Audit Committee Charter, accessed 9/28/2017.

3 Equifax Technology Committee Charter, accessed 9/27/2017.

While we recognize that some time may have been needed to assess the full extent of the breach, we believe that had the members of the Audit Committee and the Technology Committee been better informed of the challenges to the company's technological infrastructure, the company's response would have been less haphazard. McKinley, as Committee Chair, Templeton and Feidler, as members, all served on the Technology Committee since its inception in 2010, and were all well positioned to have anticipated the need for a coherent cybersecurity response plan. McKinley, having been on both the Audit Committee and the Technology Committee, also should have been able to provide an assessment of the company's risk management plans, but according to last year's proxy lacked such experience.[4] All three directors appear to have failed to anticipate the need for an adequate crisis management plan, as effectuated by Equifax's delayed and mishandled response.

The Audit Committee Failed to Provide Oversight of the Company's Legal and Compliance Obligations

Prior to the data breach, former CEO and Chair Smith had taken the unusual step of delegating his responsibility of oversight of cybersecurity risks to the company's Chief Legal Officer, John Kelley. As a result, the company's former Chief Security Officer reported directly to Kelley, who was also responsible for discharging the company's insider trading policy. An internal board investigation found no indication of insider trading among the four executives who sold $1.8 million shares in early August, but as of November 2017 the SEC continued to investigate this issue. In March 2018, civil and criminal charges of insider trading were filed against an additional former executive, who was offered the position of Chief Information Officer in the wake of the data breach.

As the committee charged with oversight of the company's legal and compliance programs, the Audit Committee should have recognized the weaknesses of the company's insider trading policies. We worry that the delegation of the cybersecurity oversight to the chief legal officer may have been inappropriate given that it is unclear what experience Mr. Kelly had with cybersecurity issues. It also remains unclear whether Mr. Kelley could have used his discretion to refuse the trades based on his knowledge of the cybersecurity breach, and what information he had at the time he authorized the trades. While we recognize that the company has since adjusted their management reporting structure so that the new Chief Information Security Officer will report directly to the CEO and that the company may now take into account cybersecurity events in deciding to halt trading, this appears to be yet another example of how the Audit Committee failed at providing the requisite level of oversight over the company's legal, regulatory and compliance obligations.

---

4 We note that according to the 2017 Board Skills Matrix, director McKinley lacked "risk management" experience; however, in the 2018 Board Skills matrix he is now listed as holding this key skill. We worry that this discrepancy may be indicative of the company applying a "check the box" exercise to its Board Skills Matrix.

Conclusion

Equifax has incurred billions in losses associated with inadequate risk management practices and internal controls. The company and Board had multiple warning signs of its weak cybersecurity practices, yet appears to have turned a blind eye to the potential threats that were presented. Despite these failures, the Board has seen fit to keep on the most tenured directors serving on the committees responsible for overseeing risk management and cybersecurity matters. In order to restore accountability and effective board oversight of key functions, **we urge you to vote AGAINST directors McKinley, Templeton and Feidler at Equifax's annual meeting on May 3, 2018.**

Please contact my colleague Tejal K. Patel at tejal.patel@ctwinvestmentgroup.com with any questions.

Sincerely,

Dieter Waizenegger

Executive Director, CtW Investment Group

This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card as it will not be accepted.