CtW Investment Group

October 18, 2017

Chairman Mark Feidler
Equifax Inc.,
c/o Corporate Secretary,
1550 Peachtree Street, N.W.
Atlanta, Georgia 30309

Dear Chairman Feidler,

The September 7th disclosure by Equifax Inc. (the "Company") that a recent data security breach compromised over 145 million Americans' personal information is evidence of the Company's failed cybersecurity processes. Despite being in the business of collecting, storing, and commercializing personal data, the haphazard response to the data breach indicates that the Board of Directors did not anticipate a core concern to the Company's operations. In doing so, it appears as though the Board and management gave little thought to preserving Equifax's most important asset – its reputation as a credit reporting agency.

Although CEO/Chairman Richard Smith, Chief Security Officer Susan Mauldin, and Chief Information Officer David Webb, retired recently, we believe that more significant steps must be taken to effectively manage the reputational crisis facing the Company. In light of these concerns, the Board should expeditiously implement the following:

- Permanently separate the CEO and Chairman positions to provide better Board oversight of management.
- Replace the Chairman of the Audit Committee, Robert Daleo, and Chairman of the Technology Committee, John McKinley, as the directors with the responsibilities most germane to the current crisis and the Company's inadequate response.
- Revise the Company's clawback policy to allow the Board to recoup executive compensation for financial and reputational damage to the Company based not only on executive misconduct, but also supervisory failures, with disclosure to shareholders of any recoupment.
- Include legal claims, settlements, and costs related to the data breach in performance measures used to determine executive compensation.
- Have the Special Committee of directors formed in response to the data breach (a) evaluate the financial impact of the breach on the Company, (b) review the Company's cybersecurity response plans, and (c) ensure that any future breaches are escalated to the Board level. The Company should also disclose to shareholders the Committee's findings.
- Establish a multi-stakeholder advisory council specializing in data security and composed of outside issue-area experts and stakeholder advocates to address the public policy concerns related to the Company's data security practices.

If the Board fails to act decisively to stem the damage from the cybersecurity breach, including the steps outlined above, we may be unable to support the re-election of directors at next year's annual meeting.

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 the Company.

Equifax's poor Board risk oversight practices may lead to serious reputational consequences

The Board's actions over the last month imply that Equifax's directors neglected to grasp the materiality of the data breach to both consumers and its shareholders. The Company failed to install a patch in response to a known data security lapse that was identified on March 7, 2017. Not only did the Company then neglect to discover the network breach that took place from May 13, 2017 through July 29, 2017, disclosure to shareholders and consumers took over a month. The remedies offered to consumers also demonstrate a surprising lack of foresight on the part of the Company, from redirecting consumers to spam sites to initially forcing consumers that signed up for the Company's own free credit monitoring to waive their right to sue Equifax. In addition, the Department of Justice in conjunction with the SEC has launched an insider trading investigation of three Company executives, including the Chief Financial Officer and the President of U.S. Information Services, for the sale of almost $1.8 million in shares, approximately two weeks after the data breach was discovered. These facts, taken as whole, indicate the ineffectiveness of the Company's policies and a culture of noncompliance.

As investors, we are extremely concerned over the potential legal and regulatory costs of a data breach of this magnitude. The Target data breach in 2013, where 40 million credit card and debit card numbers were stolen, resulted in an overall cost of $202 million, with some settlements only being finalized in the spring of 2017. At the time, the Target hack was considered to be one of the largest security breaches of consumer information. By comparison, more Americans have had their personal data compromised by Equifax than the total number of households in the United States according to the 2016 U.S. census.

The financial costs of defending numerous lawsuits and investigations over the span of several years are likely to have a far reaching impact on the long-term sustainability of the Company's performance and its product offerings. We have already seen the impact of the data breach on the short-term stock price of the Company, with the stock price dropping 35% after the announcement, a loss of approximately $6 billion in market cap to shareholders. Further, Equifax is highly leveraged, with almost $2.8 billion in debt and a debt to equity ratio that is twice that of other professional service industry companies. As such, we urge the Board to take the remedial steps outlined below.

The Board should permanently separate the CEO and Chairman positions

While we recognize the recent retirement of the Company's CEO and Chairman and appointment of Paulino Barros as interim-CEO and former Lead Independent Director Mark Feidler as Non-Executive Chairman, the cybersecurity failures demonstrate a need to restore credibility to the Company's management and Board. We have serious reservations about the fact that the full board was not told of a breach of this size until almost one month after its discovery. Further, the abrupt departure of CEO and Chairman Smith and subsequent appointment of Chairman Feidler, who was also a member of the Technology Committee during the time period when the cybersecurity breach took place, exhibits the need for greater succession planning at both the board and management level. Implementing a permanent separation of the Chairman and CEO positions would not only ensure that the Board is providing independent oversight over management, but show commitment to restoring the Company's corporate integrity and reputation over the long-term.

The Board should replace the Audit Committee and Technology Committee chairmen

The scope of the breach coupled with the delayed disclosure to shareholders requires board-level accountability, beyond the aforementioned retirement. As Chairman of the Audit Committee, Robert Daleo is charged with ensuring that the Company's disclosures regarding internal controls and material weakness are accurate, reviewing the Company's risk assessment and risk management policies, and providing oversight of the Company's regulatory compliance program. As Chairman of the Technology Committee, John McKinley is responsible for identifying trends in technology that may impact the Company's business operations, including threats resulting from disruptive technologies, as well as reviewing the Company's infrastructure as it relates to information security risk management. Given the events that have taken place during their tenure as chairs of these two committees, it is clear that the Company's internal controls and risk oversight and response plans to cybersecurity attacks are in need of serious overhaul. The Board should replace Mr. Daleo and Mr. McKinley to provide an independent review of the Company's cybersecurity and risk management systems.

The Board should adopt a robust clawback policy

We believe the Company's clawback policy does not provide an effective mechanism to address the Company's current reputational crisis. The Company should revise its clawback policy to allow for recoupment of executive compensation not only in the event of a material restatement, but also in the event of conduct that results in significant financial or reputational harm to the Company, with disclosure to shareholders in the event of any recoupment. Such conduct should include if an executive failed to fulfill any supervisory duties.

The Company has already stated that former CEO and Chair Smith will not be receiving his 2017 bonus or severance payment. That is a very limited response to the crisis in which Equifax now finds itself, and it underscores the weakness of the Company's policy on clawbacks of executive compensation. The response by Wells Fargo last year provides a good contrast, where a robust clawback policy allowed the board to respond to a crisis that badly damaged the company's reputation by clawing back $75 million in compensation from senior executives. Equifax, however, does not have such a policy. Instead, the Company's current policy appears to limit recoupments to a material financial restatement, not situations where the Company and its reputation can be badly damaged. In addition, any monies recouped under the current policy may not be disclosed to shareholders. Permitting the Company's CEO and Chairman, as well as the Chief Security Officer and Chief Information Officer, to retire with their compensation packages largely in-tact gives the impression that investors will ultimately bear the cost for the data breach, not the executives responsible for creating a strong cybersecurity defense system for the Company.

The Board should include legal claims, settlements, and associated costs of the breach into performance metrics

The potential legal and regulatory fallout from the Company's announced data breach is stunning. The Company has faced Congressional inquiries by the Senate Banking Committee, the Senate Judiciary Committee, the House Energy and Commerce Committee, and the House Financial Services Committee, as well as pending investigations from the Consumer Financial Protection Bureau and the Federal Trade Commission related to the data security breach. In addition, hundreds of lawsuits have been filed thus far, including one lawsuit from one bank claiming damages related to the cancelling and reissuing of credit cards and the cost of absorbing such losses. Further, the Company faces an insider trading investigation related to three Equifax executives.

The Company has already told investors that the costs of the data breach, and associated insurance reimbursements, will be treated as non-GAAP items as part of their presentation of adjusted earnings per share (EPS) and EBITDA margin. In a review of the Company's executive compensation practices, the *New York Times* reported that the Company also excludes the costs of legal claims and settlements in its performance measures, under its adjusted EPS metric.[1] The use of adjusted EPS, a non-GAAP measure, as a performance metric presents a distorted representation of the Company's earnings and can facilitate larger awards to executives. Further, compensation metrics are intended to reflect the Board's expectations of employee behavior and decision-making, and exclusion of adverse litigation costs, settlements, payments and fines suggest a misalignment between risks and rewards to executives. Given the significant legal liabilities and costs that are likely to follow as a result of the cybersecurity breach, the Board should immediately move to include these charges in its executive compensation performance metrics.

The Special Committee of Directors should evaluate specific issues related to the breach and disclose its findings

On September 26, the Company announced that it had created a Special Committee of directors to address the various issues that have arisen from the cybersecurity breach. The Board has failed to disclose to shareholders which directors are sitting or are assigned to this committee, whether the committee has access to cybersecurity experts, and whether the findings of the committee will be disclosed to shareholders.

We ask that the Board empower the Special Committee, if it has not done so already, to (a) evaluate the impact of the data security breach on the Company's financial stability, including possible implications for any service contracts with institutional lenders and banks that may be at risk; (b) review Equifax's response plans to anticipate cybersecurity risk, and (c) help to ensure that future data security breaches will be escalated to senior executives and the Board with follow-up. Further, the Special Committee should have access to independent financial and cyber security experts. Lastly, the Company should disclose the Special Committee's findings to shareholders. Shareholders would benefit from greater transparency and insight into the Board's evaluation of the Company's cybersecurity compliance programs. Similar disclosures were provided by Yahoo, following public outcry over its data security breaches in 2013 and 2014.

The Board should establish a multi-stakeholder advisory committee to address data security issues

One of the core components to former CEO and Chairman Richard Smith's business strategy was to obtain as much personal information as possible that could then be repackaged and sold to Equifax customers, which often times are institutions or businesses and not end-consumers. As a result, consumer information, which is generally not even given to the Company directly by individuals, has become a cornerstone of its new product lines over the last decade, particularly in the areas of human resources and payroll information.

The recent public response to the data breach demonstrates the need for greater communication between the Company and consumers. The Board should establish a multi-stakeholder advisory council composed of outside issue-area experts and stakeholder advocates specializing in data security,

[1] Gretchen Morgenson, "Consumers, but not Executives, May Pay for Equifax Failings," *New York Times*, September 13, 2017, *available at* https://www.nytimes.com/2017/09/13/business/equifax-executive-pay.html?mcubz=3.

including consumer advocate groups, banking and credit union representatives, data security experts, and academics. The advisory council would: (a) meet regularly with management and the Board; (b) serve as a point of contact for external and internal stakeholders to raise concerns regarding data security breaches; and (c) assist in overseeing the Company's monitoring of community engagement, stakeholder relationships, and corporate reputation. We believe that the establishment of this council will provide an effective mechanism to generate feedback, communication, and an ongoing dialog between the Company and the public.

Conclusion

Equifax plays a critical role in the nation's financial system, and it is imperative that its own credibility be restored. As Equifax faces the legal, financial, and reputational challenges related to its data breach, investors worry that the Board is inadequately equipped to respond to an issue that has impacted almost 45% of the U.S. population. We urge the Board to commit to the changes outlined above and encourage a dialogue with its shareholders as to how best to address the significant business risks facing the Company. We would be happy to discuss our recommendations with you at your convenience. Please contact my colleague Tejal K. Patel at (202) 721-6079 to pursue such a discussion.

Thank you.

Dieter Waizenegger
Executive Director