Investor Relations Q&A, Equifax Cybersecurity Incident

September 7, 2017

1. **What happened?**
   We identified a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. We discovered the unauthorized access and acted immediately to stop the intrusion. We promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. We also reported the criminal access to law enforcement and continue to work with authorities.

2. **When did the company learn of this incident?**
   We learned of the incident on July 29, 2017, and acted immediately to stop the intrusion and conduct a forensic review.

3. **Over what period of time did the unauthorized access occur?**
   Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.

4. **What information may have been impacted?**
   The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Criminals also accessed credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers. As part of our investigation of this application vulnerability, we also identified unauthorized access to limited personal information for certain UK and Canadian residents. We have found no evidence that personal information of consumers in any other country has been impacted.

5. **Are Equifax's core consumer or commercial credit reporting databases impacted?**
   We have found no evidence of activity on Equifax's core consumer or commercial credit reporting databases.

6. **Is the issue contained?**
   Yes, this issue has been contained.

7. **What are you doing to prevent this from happening again?**
   Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

8. **What are the features offered in TrustedID Premier?**
   TrustedID Premier provides you with copies of your Equifax credit report; the ability to lock your Equifax credit report; 3-Bureau credit monitoring of your Equifax, Experian and TransUnion credit reports; Internet scanning for your Social Security number; and identity theft insurance.

9. **Do you have an estimate of the costs you expect to incur related the cybersecurity incident, including timing? Does Equifax have cyber insurance and to what extent will it offset the financial impact of this incident?**
   At this time, it is too early for us to provide specific estimates of the costs we expect to incur related to the cybersecurity incident. The most significant near-term costs expected to be incurred will be delivering our TrustedID Premier identity theft protection and credit file monitoring product for a period of 12 months to consumers who enroll. In addition, Equifax will incur legal, forensic consulting and other costs related to the incident. Equifax carries cybersecurity, crime, general liability and other lines of insurance, and we have begun discussions with our carriers regarding the incident.

10. **How will you disclose the costs related to the cybersecurity incident in your financial statements and public filings?**
    Equifax will separately disclose costs specifically related to this cybersecurity incident, as well as any insurance reimbursements that offset these costs. These costs and reimbursements will be treated as non-GAAP items in our presentation of Adjusted EPS and Adjusted EBITDA margin. The timing of the accrual for or incurrence of related costs may differ from the timing of recognizing insurance reimbursement for those costs.

11. **Do you expect this cybersecurity incident to impact your long term financial model?**
    Equifax remains committed to delivering on the long term financial model of 7-10% revenue growth and 11%-14% growth in Adjusted EPS on average over a business cycle. Equifax's long term financial model reflects our continuing fundamental ability to utilize our unique and differentiated data assets and leading analytical capability to deliver high value products and services to our customers.

12. **Are you expecting any near term impact to your financial results from the cybersecurity incident?**
    We do expect some disruption to our business, as we focus on completing the detailed investigation of this event, taking the steps needed to minimize the likelihood that this type of incident will happen again, and working with customers to address their concerns and maintain their trust as a leading supplier of consumer data and analytics. We also expect impacts to our Global Consumer business as it focuses on delivering TrustedID Premier to US consumers. We will provide a further update on our 3Q17 earnings call in October.

13. **Does this cybersecurity incident impact your capital allocation priorities going forward?**
    Our capital allocation priorities are unchanged at this time. As we have previously indicated, our investment priorities in order of importance are: (1) internal investment; (2) dividends; (3) acquisition; and (4) share repurchase. We do, however, expect to increase our capital spending in an effort to further accelerate IT infrastructure, systems and data security and resiliency improvement actions.

14. **When was the Board made aware of the incident? What has their involvement been?**
    We promptly informed the Board upon learning the potential scope of the incident and have engaged them since then in regular discussions.

15. **Are you still planning to attend sell-side conferences scheduled for the remainder of the year?**
    Yes, investors are an important constituency and we intend to continue a high level of accessibility and participation in conferences, NDR's and other meeting requests.