Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

ATLANTA, September 15, 2017 -- As part of the company's ongoing review of the cybersecurity incident announced September 7, 2017, Equifax Inc. (NYSE: EFX) today made personnel changes and released additional information regarding its preliminary findings about the incident.

The company announced that the Chief Information Officer and Chief Security Officer are retiring. Mark Rohrwasser has been appointed interim Chief Information Officer. Mr. Rohrwasser joined Equifax in 2016 and has led Equifax's International IT operations since that time. Russ Ayres has been appointed interim Chief Security Officer. Mr. Ayres most recently served as a Vice President in the IT organization at Equifax. He will report directly to the Chief Information Officer. The personnel changes are effective immediately.

Equifax's internal investigation of this incident is still ongoing and the company continues to work closely with the FBI in its investigation.

Specific Details of Incident:

- On July 29, 2017, Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. In response, the Security team investigated and blocked the suspicious traffic that was identified.
- The Security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, the company took offline the affected web application that day.
- The company's internal review of the incident continued. Upon discovering a vulnerability in the Apache Struts web application framework as the initial attack vector, Equifax patched the affected web application before bringing it back online.
- On August 2, 2017, Equifax contacted a leading, independent cybersecurity firm, Mandiant, to assist in conducting a privileged, comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted.
- Over several weeks, Mandiant analyzed available forensic data to identify unauthorized activity on the network.
- The incident potentially impacts personal information relating to 143 million U.S. consumers – primarily names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.
- In addition, 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, were accessed.
- Equifax also identified unauthorized access to limited personal information for certain U.K. and Canadian residents and is working with regulators in those countries.
- With respect to the company's security posture, Equifax has taken short-term remediation steps, and Equifax continues to implement and accelerate long-term security improvements.

Questions Regarding Apache Struts:

· The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.
· Based on the company's investigation, Equifax believes the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017.
· The particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017.
· Equifax's Security organization was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems in the company's IT infrastructure.
· While Equifax fully understands the intense focus on patching efforts, the company's review of the facts is still ongoing. The company will release additional information when available.

Overview of Consumer Support Response and Recent Developments

The company is fully committed to proactively supporting consumers who may have been impacted by the cybersecurity incident. A timeline of our response includes:

· The company worked diligently with Mandiant to determine what information was accessed and identify the potentially impacted consumers in order to make an appropriate public disclosure of the incident.
· As soon as the company understood the potentially impacted population, a comprehensive support package was rolled out to consumers on September 7, 2017.
· Equifax took the following steps:
○ Created a dedicated website where consumers could understand whether they were impacted, find out more information about the incident and learn how to protect themselves.
○ The company offered free credit file monitoring and identity theft protection to all U.S. consumers, regardless of whether they were definitively impacted.
· TrustedID Premier includes 3-Bureau credit monitoring of Equifax, Experian, and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers.
○ The company has also set up a dedicated call center to assist consumers with questions and signing up for the free offering and has continued to ramp up the call center to reduce wait times.
    - Equifax also provided written notification to all U.S. State Attorneys General and contacted other federal regulators.

· Since the announcement, Equifax has taken additional actions including:
○ Providing a more prominent and clear link from the main www.equifax.com website to the cybersecurity incident website www.equifaxsecurity2017.com, so that consumers can quickly and easily find the information they need.
        - Tripling the call center team and continuing to add agents, despite facing some difficulty due to Hurricane Irma.

○ Resolving issues with the impact look-up tool.
○ Addressing confusion concerning the arbitration and class-action waiver clauses included in the Terms of Use applicable to the product:
· The company never intended for these clauses to apply to this cybersecurity incident.

· Because of consumer concern, the company clarified that those clauses do not apply to this cybersecurity incident or to the complimentary TrustedID Premier offering.
· The company clarified that the clauses will not apply to consumers who signed up before the language was removed.
○ Clarifying that no credit card information is required to sign up for the product and that consumers will not be automatically enrolled or charged after the conclusion of the complimentary year.
○ Making changes to address consumer concerns regarding security freezes:
· The company clarified that consumers placing a security freeze will be provided a randomly generated PIN.
· The company continues to work on technical difficulties related to the high volume of security freeze requests.
· Consumers who paid for a security freeze starting at 5pm EST on September 7, 2017 will receive a refund.
· The company agreed to waive fees for removing and placing security freezes through November 21, 2017.

About Equifax

Equifax is a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions. The company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.

Headquartered in Atlanta, Ga., Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX. Equifax employs approximately 9,900 employees worldwide.