

**UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION**  
Washington, D.C. 20549

**FORM 8-K**

**CURRENT REPORT**

Pursuant to Section 13 or 15(d) of the  
Securities Exchange Act of 1934

Date of report (Date of earliest event reported): September 7, 2017

**EQUIFAX INC.**

(Exact name of registrant as specified in Charter)

**Georgia**

(State or other jurisdiction  
of incorporation)

**001-06605**

(Commission File  
Number)

**58-0401110**

(IRS Employer  
Identification No.)

**1550 Peachtree Street, N.W.  
Atlanta, Georgia**

(Address of principal executive offices)

**30309**

(Zip Code)

Registrant's telephone number, including area code:**(404) 885-8000**

**Not Applicable**

(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligations of the registrant under any of the following provisions:

- Written communication pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
- Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

- Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

- If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.
-

**Item 8.01. Other Events.**

On September 7, 2017, the Company issued a press release providing important information regarding a cybersecurity incident involving access to certain consumer information. A copy of the press release is attached hereto as Exhibit 99.1 and is incorporated by reference herein.

**Item 9.01. Financial Statements and Exhibits.**

(d) Exhibits

99.1 Press release of Equifax Inc. dated September 7, 2017.

---



## Exhibit Index

The following exhibit is being filed with this report:

<u>Exhibit No.</u>	<u>Description</u>
99.1	<a href="#">Press release of Equifax Inc. dated September 7, 2017.</a>



For Immediate Release  
September 7, 2017

## **Equifax Announces Cybersecurity Incident Involving Consumer Information**

### **No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases**

### **Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers**

Equifax Inc. (NYSE: EFX) today announced 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. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes 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. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company 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. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called 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 - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com) or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. - 1:00 a.m. Eastern time.

---

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.

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.

CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."

### **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.

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.

### **Forward-Looking Statements**

This release contains forward-looking statements and forward-looking information. These statements can be identified by expressions of belief, expectation or intention, as well as estimates and statements that are not historical fact. These statements are based on certain factors and assumptions with respect to the investigation of the cybersecurity incident to date. While the company believes these factors and assumptions to be reasonable based on information currently available, they may prove to be incorrect.

Several factors could cause actual results to differ materially from those expressed or implied in the forward-looking statements, including, but not limited to, the final results of the investigation, including the final scope of the intrusion, the type of information accessed and the number of consumers impacted. A summary of additional risks and uncertainties can be found in our Annual Report on Form 10-K for the year ended December 31, 2016, including without limitation under the captions "Item 1. Business -- Governmental Regulation" and "-- Forward-Looking Statements" and "Item 1A. Risk Factors," and in our other filings with the U.S. Securities and Exchange Commission. Forward-looking statements are given only as at the date of this release and the company disclaims any obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.

### **Contacts:**

Ines Gutzmer  
Corporate Communications  
mediainquiries@equifax.com  
404-885-8555