Sep 07, 2017

No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases. Equifax to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers

ATLANTA, Sept. 7, 2017 /PRNewswire/ -- 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 [also tax identification numbers (IRS ID in lieu of SSN), email addresses, and additional license information. See update above.] 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. [Canadians and British citizens.] 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."

Commented [TML1]: population of USA = 323 M
children (<18) = 74 M
Adults = 249 M
Equifax 145.5 M or 58% of adults in USA

Commented [TML2]: Just because a website is publicly and anonymously available, criminals should not exploit it. Bad criminals!
Just because I left the boxes for my new 86" 4K TV, home theatre audio, and all those white Apple boxes on the curb in front of my house, and just because I didn't lock any of the doors, and just because we all went away for the day…doesn't mean criminals should exploit my front door.

Commented [TML3]: 7 weeks while security was breached.
It took from July 29 to Sept 7, i.e. 1 month, 1 week, 2 days, to announce that 57% of the USA adult population was at financial risk. The time it takes for stolen credentials & credit card numbers to be purchased after being made available on the dark web: 9 minutes.

Commented [TML4]: Was their search for evidence of unauthorized activity as thorough and competent as their security?

Commented [TML5]: Plenty for identity theft

Commented [TML6]: Acted immediately? The fix for the Apache Struts vulnerability was made available to the world in March.

Commented [TML7]: "disappointing"? Disappointment for these guys is wanting a Lamborghini convertible but having to settle for a Ferrari coupe.

Equifax has established a dedicated website, 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.comor 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.

Commented [TML8]: This site was put online with another security vulnerability.

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

View original content:http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html

SOURCE Equifax Inc.

Back to News 2017

Powering the World with Knowledge™

September 11th, 2017 update: Equifax data breach could cost the international credit rating company hundreds of millions of dollars in direct damages. This is just on what Heidi Shey, a senior security and risk analyst at Forrester Research, calls measurable damages, such as regulatory fines, possible damages awarded by courts, new security and audit measures needed to be implemented and credit monitoring offered to victims.

September 26th, 2017 update: CEO, CIO and CISO 'retire'. Equifax admitted its IT staff *did know* a patch was available in March for the vulnerability that led to the breach, though for some reason it wasn't fixed for 19 weeks. That the patch was not addressed for that long indicates some kind of IT mgmt. disfunction (e.g. insufficient resources, discipline, record keeping) and that there were no security layers between their confidential data and the Apache Web Server which indicates IT architecture, integrity, and security design incompetence. E.g. a bug in creating an SQL statement run through a PHP script accessing the DB could cause data loss. And that's just shooting yourself in the foot let alone allowing others to get through your web server and shoot you in the chest.

February 12, 2018 update: "Since the breach, the company has been accused of persistently botching its response. Not only did Equifax take four months to disclose the hack, the breach was later attributed to a vulnerable server that the company had failed to patch earlier in the year. After the hack was eventually disclosed, Equifax struggled to inform its users -- many of which had no idea the company was hoarding data on them in the first place -- if they were vulnerable."

The irony of not taking your own advice:

Corporate Data Breach Assistance | Equifax

"Help protect your reputation by acting quickly…"

"Corporate Data Breach Assistance empowers you to respond to a data breach in a timely in order to minimize the impact to your business, brand, and your customers."

https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

About Us > Investor Relations > News and Events > News > 2017

Equifax Announces Cybersecurity Incident Involving Consumer Information

- Financial Information
- News and Events
- Stock Information
- Stockholder Services
- Contact Us

March 2, 2018 update: Equifax data breach could become the most costly in corporate history. "well over USD$600-million" and has shed 20% of its value since Sept. 7 2017 wiping out $2.9B in Market Cap.

March 15th, 2018 update**:** The former CIO of credit reporting agency Equifax has been charged with insider trading. "The SEC alleges that before Equifax's public disclosure of the data breach, Jun Ying, former CIO, exercised all of his vested Equifax stock options and then sold the shares, reaping proceeds of nearly $1 million. By selling before public disclosure of the data breach, Ying avoided more than $117,000 in losses," the SEC's complaint alleges. Four other executives also sold shares at that time.

Search: equifax class action lawsuit

e.g. http://securities.stanford.edu/filings-documents/1063/EI00_15/2019128_r01x_17CV03463.pdf