March 1, 2018

Equifax Releases Updated Information on 2017 Cybersecurity Incident

ATLANTA, March 1, 2018 /PRNewswire/ -- As a result of ongoing analysis of data stolen in last year's cybersecurity incident, Equifax Inc. (NYSE: EFX) today announced that the company has confirmed the identities of U.S. consumers whose partial driver's license information was taken. Equifax was able to identify these consumers by referencing other information in proprietary company records that the attackers did not steal, and by engaging the resources of an external data provider.

Through these additional efforts, Equifax was able to identify approximately 2.4 million U.S. consumers whose names and partial driver's license information were stolen, but who were not in the previously identified affected population discussed in the company's prior disclosures about the incident. This information was partial because, in the vast majority of cases, it did not include consumers' home addresses, or their respective driver's license states, dates of issuance, or expiration dates.

The methodology used in the company's forensic examination of last year's cybersecurity incident leveraged Social Security Numbers (SSNs) and names as the key data elements to identify who was affected by the cyberattack. This was in part because forensics experts had determined that the attackers were predominately focused on stealing SSNs. Today's newly identified consumers were not previously informed because their SSNs were not stolen together with their partial driver's license information.

"This is not about newly discovered stolen data," said Paulino do Rego Barros, Jr., Interim Chief Executive Officer. "It's about sifting through the previously identified stolen data, analyzing other information in our databases that was not taken by the attackers, and making connections that enabled us to identify additional individuals."

Equifax will notify these newly identified U.S. consumers directly, and will offer identity theft protection and credit file monitoring services at no cost to them. Information about registering for these services will be included in the notification.

"We continue to take broad measures to identify, inform, and protect consumers who may have been affected by this cyberattack," Barros added. "We are committed to regaining the trust of consumers, improving transparency, and enhancing security across our network."

As the company committed to do, Equifax launched Lock & Alert™ to all U.S. consumers on January 31. This new service, which is free for life, enables consumers to quickly lock and unlock their Equifax credit report using a computer or app downloaded on their mobile device.

Importantly, the company's forensics experts have found no evidence that Equifax's core consumer, employment and income, or commercial credit reporting databases were accessed as part of the cyberattack, and the company believes it will have met all applicable requirements to notify consumers.

Since announcing this incident, Equifax has taken steps to communicate with and assist consumers and customers. Among other things, the company has established a web portal advising U.S. consumers to review their account statements and credit reports, identify any unauthorized activity, and protect their personal information from further attack. Additionally, the company offered free identity theft protection and credit file monitoring services to all U.S. consumers regardless of whether or not they were impacted.

Consumers can visit www.equifaxsecurity2017.com for more information about the cybersecurity incident and for answers to frequently asked questions.

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 statements that are not historical fact. Several factors could cause actual results to differ materially from those expressed or implied in the forward-looking statements, including additional analysis of the data stolen; the government investigations and litigation resulting from the 2017 cybersecurity incident; and the response of government regulators to the 2017 cybersecurity incident including the updated information included in this release; and the possibility that new information may arise or different conclusions are reached on such new information. A summary of additional risks and uncertainties can be found in our Annual Report on Form 10-K 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.

About Equifax

Equifax is a global information solutions company that uses 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 10,300 employees worldwide.

FOR MORE INFORMATION

MediaInquiries@equifax.com

View original content with multimedia:http://www.prnewswire.com/news-releases/equifax-releases-updated-information-on-2017-cybersecurity-incident-300606609.html

SOURCE Equifax Inc.