Equifax provides details on 2017 data breach - 8-K (17:25 ET)
Wednesday, May 09, 2018 02:38:47 AM (GMT)

- On 4-May, Equifax Inc. submitted a statement for the record to multiple Congressional committees regarding the cybersecurity incident announced on 7-Sep-17 in which certain personally identifiable information of U.S. consumers was stolen. The statement provided additional detail on the data elements stolen in the cybersecurity incident related to those U.S. consumers and was made in response to, and as part of the company's ongoing cooperation with, governmental requests for information. The additional detail provided in the statement, which is described below, does not identify additional consumers affected and does not require additional consumer notifications.
    - Detail on Documents Uploaded to Online Dispute Portal
        - As part of the company's notification of affected consumers in 2017, the company notified by direct mail the consumers who had uploaded dispute documents to the company's online dispute portal that their dispute information was accessed, and in order to provide information to each consumer regarding his or her accessed images, the company provided each consumer with a list of the specific files that he or she had uploaded onto the company's online dispute portal and the dates of those uploads. Because the company directly notified each impacted consumer, the company had not previously analyzed the government-issued identifications contained in the images uploaded in the dispute portal.
        - In response to governmental requests for additional information, the company recently analyzed the dispute documents stolen in the cybersecurity incident and determined the approximate number of valid U.S. government-issued identifications that had been uploaded to the dispute portal: 38,000 driver's licenses, 12,000 social security or taxpayer ID cards, 3,200 passports or passport cards and 3,000 other government-issued identification documents such as military IDs, state-issued IDs and resident alien cards. The government identification documents described above do not identify additional consumers affected. Since all of these consumers were previously notified of the specific files that he or she had uploaded to the dispute portal, no further notifications of consumers are required.
    - Detail on Data Elements
        - In addition to the company's review of the dispute documents, in order to respond to governmental requests for additional information, the company provided additional information regarding the approximate number of consumers impacted for each of the data elements that was stolen in the cybersecurity incident.
        - The attackers stole consumer records from a number of database tables with different schemas. With assistance from Mandiant, a cybersecurity firm, forensic investigators were able to standardize certain data elements for further analysis to determine the consumers whose personally identifiable information was stolen. As a result of its analysis of the standardized data elements, including using data not stolen in the cybersecurity incident, the company was able to confirm the approximate number of those impacted U.S. consumers for each of the following data elements stolen in the cybersecurity incident: name (146.6M), date of birth (146.6M), Social Security number (145.5M), address information (99M), gender (27.3M), phone number (20.3M), driver's license number (17.6M), email address (1.8M), payment card number and expiration date (209,000), TaxID (97,500) and driver's license state (27,000). As noted above, the additional detail provided does not identify additional consumers affected, and does not require additional consumer notifications.
- StreetAccount notes that the stock fell (2%) in after-hours trading.

Reference Links:
- SEC filing: 8-K

Industries: Business Services
Primary Identifiers: EFX-US
Related Identifiers: EFX-US

Related Stories:

- Equifax announces cybersecurity incident involving consumer information impacting 143M US consumers