GOVERNOR CUOMO AND NEW YORK ATTORNEY GENERAL LETITIA JAMES ANNOUNCE $19.2 MILLION SETTLEMENT WITH EQUIFAX OVER 2017 DATA BREACH

Department of Financial Services and New York Attorney General's Office Fine Equifax and Two Subsidiaries

DFS Investigation Found Credit Rating Agency Had Inadequate Information Security Practices, Failed to Ensure Safety of Consumer Data and Provided Insufficient Customer Service Following the Breach

Equifax to Pay up to $425 Million in Restitution, Provide New York Consumers Credit Monitoring Services, Free Annual Credit Reports for Five Years

Governor Andrew M. Cuomo and Attorney General Letitia James today announced that New York is holding Equifax Inc. accountable for the 2017 data breach that exposed the sensitive financial and personal information

of millions of Americans, including 8.5 million New Yorkers. The settlement stems from separate investigations by the Department of Financial Services and the New York Attorney General's Office into the credit rating agency and two of its subsidiaries, Equifax Information Services LLC and Equifax Consumer Services LLC. Under the settlement, the companies will pay a fine of $10 million to DFS, $9.2 million to the New York Attorney General's Office as part of $175 million to Multi-State Attorney Generals including New York, and Equifax has committed up to $425 million to the consumer restitution fund.

"Credit rating agencies have a responsibility to safeguard consumers' financial and personal information, and this egregious data breach and the agency's response was completely unacceptable," **Governor Cuomo said.** "In New York we are sending a clear message to these agencies that they will be held accountable if they leave consumers' private data vulnerable to exposure, and we will continue our rigorous oversight of these agencies to ensure New Yorkers are protected in the future."

Attorney General Letitia James said, "Equifax put profits over privacy and greed over people, and must be held accountable to the millions of people they put at risk. This company's ineptitude, negligence, and lax security standards endangered the identities of half the U.S. population. Now it's time for the company to do what's right and not only pay restitution to the millions of victims of their data breach, but also provide every American who had their highly sensitive information accessed with the tools they need to battle identity theft in the future."

Financial Services Superintendent Linda A. Lacewell said, "First and foremost, the settlement announced today holds Equifax accountable for its egregious breach in its duty to consumers in safeguarding their sensitive personal identifying information and restores some peace of mind and protection to New Yorkers. Strengthening consumer protections for New Yorkers, DFS now requires credit rating agencies to be licensed and

supervised by DFS, and comply with the Department's landmark cybersecurity regulation to better guard against potential breaches."

In addition to the fine, Equifax will provide New York consumers with credit monitoring services and free annual credit reports, and will pay restitution to consumers affected by the breach. New York consumers who were impacted by the data breach may enroll in at least four years of credit monitoring by the three major credit-monitoring services - Equifax, Experian and Transunion - and receive two free credit reports from Equifax every 12 months for five years. Consumers will also be able to submit claims for reimbursement for certain losses resulting from the data breach to a court-appointed administrator. The program to pay restitution to consumers will be conducted in connection with settlements that have already been reached in the multi-district class action suits filed against Equifax, as well as with settlements that have been reached with the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB). Equifax will pay an additional $50 million to the CFPB.

DFS investigated the companies' security practices before and at the time of the breach, as well as their communications and the services provided to consumers immediately after announcement of the breach, and found that the companies engaged in practices that violated the Dodd-Frank Act and Financial Services Law § 408.

The DFS investigation found that the 2017 data breach at Equifax exposed New York consumers' sensitive personal information, including their full names, Social Security numbers, dates of birth, addresses and for some consumers, credit card numbers, driver's license numbers and dispute documents containing personal identifying information, and thus could have the potential to cause injury, including financial injury, to consumers and businesses.

DFS also found that following the announcement of the data breach on September 7, 2017, Equifax, Inc. and its two subsidiaries failed to provide

adequate assistance to affected consumers, including inadvertently directing consumers to a website that was not owned by Equifax; failing to alert consumers that their data had not only been accessed attackers, but stolen; and providing a data breach website that was unable to provide certainty for consumers about whether they were impacted by the breach.

DFS's findings about the companies' security practices include the following:

- The companies had inadequate information security practices, and failed initially to detect a critical vulnerability affecting their online consumer dispute portal that consumers use to dispute the completeness or accuracy of information in their credit files.
- That vulnerability related to Apache Struts, an open-source web application framework that the companies used in connection with the dispute application.
- The company's Vulnerability Assessment Team was aware that it didn't have complete visibility into where the vulnerable version of Struts was used.

During the relevant period, Equifax conducted internal and external reviews of the information security program that identified areas for improvement and failed to implement on a timely basis some security measures that were mandated by their own policies. In addition, the companies' internal documents demonstrate that they were aware they were storing personal identifying information in development and testing environments, increasing the risk of identity theft, misuse of data and fraud. The companies also failed to encrypt certain consumers' personal identifying information and failed to decrypt certain incoming and outgoing traffic in violation of their own policies.

A copy of the full consent order is available here.

The case was handled by DFS Assistant Counsel Serwat Farooq and Assistant Counsel Laura Sarli under the supervision of Deputy Superintendent for the Civil Investigations Unit Christopher B. Mulvihill and

Katherine A. Lemire, Executive Deputy Superintendent of the Consumer Protection and Financial Enforcement Division, together with Deputy Superintendent for Licensed Financial Services Wendy Henry, under the Supervision of Executive Deputy Superintendent of the Banking Division Shirin Emami.

###