

**U.S. ATTORNEY BRIAN J. STRETCH DELIVERS REMARKS AT PRESS CONFERENCE
ANNOUNCING CHARGES AGAINST RUSSIAN FSB OFFICERS AND THEIR CRIMINAL
CONSPIRATORS FOR HACKING YAHOO**

**Remarks as prepared for delivery
March 15, 2017
WASHINGTON, D.C.**

Thank you, [FBI Executive Assistant Director] Paul [Abbate]. My name is Brian Stretch. I am the United States Attorney in San Francisco. I am pleased to join the Head of the National Security Division and the Executive Assistant Director of the FBI to advise you of the criminal charges returned in connection with the widely reported Yahoo data breach which occurred in 2014.

As an important reminder, the criminal charges in the indictment announced today are allegations only and the four named defendants are presumed innocent until proven guilty.

We are joined today by the investigating AUSA, National Security Division trial lawyers, and experienced FBI agents who worked tirelessly with Yahoo and Google to identify the responsible parties and their methods and means for perpetrating one of the largest data breaches ever.

Silicon Valley is home to the world's leading technology companies. The Valley's computer infrastructure provides the means by which people around the world communicate with each other in their business and personal lives.

Everyday criminal hackers endeavor to gain unauthorized access to personal and proprietary information for nefarious purposes. The Department of Justice and the technology companies together share a common goal and responsibility to protect private communications from cyber criminals.

The privacy and security of internet-based communications must be governed by the rule of law. People rightly expect that the government and technology companies both will make every effort to ensure that communications through internet providers will remain private. Exceptions to this principle should be few and governed by statute and court order.

To this end, in recent years, the DOJ has made cyber security a top priority and has taken a number of steps to protect the public from cyber crime. Part of this effort has involved conducting extensive outreach in Silicon Valley and elsewhere to encourage service providers to report unauthorized intrusions and theft of trade secrets. Both the DOJ and the technology companies throughout the country are beginning to see the fruits of this outreach.

The benefits of reporting intrusions to the U.S. Government include:

- Obtaining assistance from the government to determine the scope and extent of the intrusion and to determine the identity of the hackers.
- Obtaining information about what use the hackers put to the stolen information.

- And by working with investigators, of course, the companies can target and limit investigatory methods so as to prevent unnecessary access to the private records of innocent victims and accountholders.

Regarding the hacks we are talking about today, Yahoo and Google informed the DOJ of the data breaches, cooperated extensively with the FBI and DOJ attorneys to investigate the intrusions, and by leveraging the combined efforts of the government and the service providers, assisted in effectuating a targeted, streamlined, and efficient investigation.

The update on this approach? The responsible parties have been identified, charges returned, one defendant has been arrested, and arrest warrants have been issued for the remaining defendants. Importantly, the cooperative efforts of the government and the private sector in this instance allowed the U.S. Attorney's Office, along with the National Security Division and the FBI to accomplish these initial results while maintaining the fundamental privacy interests of the account holders who had their information stolen.

We commend both Yahoo and Google for working with our office, the FBI, and the National Security Division lawyers to identify and seek justice for the perpetrators of these infusions.