YAHOO!

February 23, 2017

The Honorable John Thune
Chairman
Committee on Commerce,
Science and Transportation
United States Senate
Washington, DC 20510

The Honorable Jerry Moran
Chairman
Subcommittee on Consumer Protection,
Product Safety, Insurance and Data Security
United States Senate
Washington, DC 20510

Dear Chairman Thune and Chairman Moran:

I write in response to your February 10, 2017 letter to Marissa Mayer regarding the data security incidents disclosed by Yahoo! Inc. (Yahoo) in September and December 2016.

At the outset, please understand that Yahoo shares the Committee's goal of protecting consumers and their information, and we take our obligations to our users and their security seriously.

In an increasingly connected world, there has been a tremendous increase in the pace and sophistication of cyber threats. Businesses, individuals, government entities, and others have been constantly in the crosshairs of nefarious and malicious online actors, including state-sponsored actors. As you note in your letter, Yahoo was the victim of attacks by such actors, which resulted in the user notifications and security disclosures we made last year.

Through strategic proactive detection initiatives and active response to unauthorized access to user accounts, Yahoo strives to stay ahead of these ever-evolving online threats and to keep our users and platforms secure. We continue to enhance our systems to detect and prevent unauthorized access, and to strengthen our defenses against threats to security, including advanced persistent threats.

We understand the Committee's desire to learn more about what occurred and the steps Yahoo has taken to secure user accounts. We appreciate the opportunity Yahoo was given to provide a bipartisan staff briefing on September 26, 2016, just four days after the company's initial security announcement, and this opportunity to further update the Committee in writing here and in an upcoming briefing. The company is also cooperating with federal, state, and foreign governmental officials and agencies about the security incidents disclosed on September 22, 2016 and December 14, 2016, and related matters. Additionally, as we indicated in our briefing in September, the company is actively working with U.S. law enforcement authorities on these matters.

101 Constitution Avenue NW, Suite 800W Washington DC 20001
P 202 777 1054 F 202 777 1051

In the spirit of cooperation, below are responses to the Committee's questions. The company, with the assistance of outside forensic experts, continues to investigate the security incidents and related matters. We will continue to provide additional information to this Committee as available and appropriate. The information set forth below relates specifically to the company's disclosures regarding the incidents announced on September 22 and December 14, 2016. As indicated in the Form 10-Q filed with the Securities and Exchange Commission on November 9, 2016, an Independent Committee of the Board of Directors has investigated the company's contemporaneous knowledge, handling and notifications to users regarding the unauthorized access in question. The Board's Independent Committee will be providing a briefing to you and your staff on these matters.

Again, thank you for the opportunity to provide more information about our ongoing investigation into this complex matter.

Sincerely,

April Boyd
Vice President & Head of Global Public Policy

1. With respect to both the 2013 and 2014 incidents, how many users do these incidents affect? Please describe Yahoo!'s efforts to identify and provide notice to these users.

With respect to the 2013 incident that Yahoo disclosed on December 14, 2016, Yahoo believes an unauthorized third party stole from Yahoo's network certain user account information associated with more than one billion user accounts (the "2013 Incident"). With respect to the 2014 incident that Yahoo disclosed on September 22, 2016, Yahoo believes a copy of certain user account information associated with approximately 500 million user accounts was stolen from Yahoo's network by what the company believes is a state-sponsored actor (the "2014 Incident"). A majority of the user accounts that were potentially affected by the 2014 Incident also are believed to have been affected by the 2013 Incident.

Yahoo also disclosed in its Form 10-Q filed on November 9, 2016 and in its December 14, 2016 press release that it was investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the investigation, Yahoo has identified user accounts for which the company believes forged cookies were taken or used in 2015 and 2016. Yahoo has connected some of this activity to the same state-sponsored actor believed to be responsible for the 2014 Incident.

Yahoo worked closely with leading outside forensic experts to investigate these issues and identify the potentially affected user accounts.

Yahoo notified potentially affected account holders by email, upon login and through in-product messaging. To the extent a user account was potentially affected by more than one incident, Yahoo sent the account holder separate notices about each incident. In addition, for each incident, Yahoo posted a notice on its website, issued a press release, and created a Security Issue FAQs page (at yahoo.com/security-update) with additional information about the particular issue and security resources for users.

2. With respect to the aforementioned incidents, what type of data does Yahoo! believe to have been compromised? Does the data include sensitive personal information?

With respect to the 2013 Incident and 2014 Incident, the stolen account information included names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information did not include clear text passwords, payment card data, or bank account information. Payment card data and bank account information are not stored in the system that either investigation found to be affected.

With respect to the cookie forging activity, Yahoo's systems would recognize a forged cookie as indicating a valid user in a logged-in state, thereby allowing an intruder to bypass the need for a password to access a user's account. Yahoo has invalidated the forged cookies so they cannot be used to access users' accounts.

3. What steps has Yahoo! taken to identify and mitigate potential consumer harm associated with these incidents?

Incident-Specific Responses

As indicated in the response to question 1 above, Yahoo notified potentially affected users by email, upon login, and through in-product messaging. On September 22, 2016 and December 14, 2016, for each incident, Yahoo also posted a notice on its website, issued a press release, and created a Security Issue FAQs page with additional information about the issue and security resources for users. The notice on the website and FAQs remain active today.

Out of an abundance of caution, Yahoo is requiring any users who have not changed their passwords since late 2014 to do so, and has asked users to ensure Yahoo has an up-to-date alternative means of account verification. Yahoo also invalidated unencrypted security questions and answers so they cannot be used to access user accounts.

Yahoo has encouraged users to review all of their online accounts for suspicious activity and to change their passwords and security questions and answers for any other accounts on which they use the same or similar information used for their Yahoo account. The company further recommended that users avoid clicking links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information. Additionally, the company has asked that users consider using Yahoo Account Key

(at login.yahoo.com/accountkey/setup), a simple authentication tool that eliminates the need to use a password on Yahoo altogether.

With respect to the cookie forging activity, Yahoo has taken various steps to address this issue, including:

- Rejecting and blocking forged cookies that have been identified;
- Invalidating forged cookies by enhancing and modifying the code and algorithms used to create cookies; and
- Creating customized alerts and monitoring tools to help detect the attempted use of forged cookies.

Ongoing Focus on User Security

In addition to the company's incident-specific responses, over the course of Yahoo's more than 20-year history, the company has focused on and invested in security programs and personnel to protect users. After CEO Marissa Mayer joined the company, she hired a new Chief Information Security Officer and approximately doubled the staff of Yahoo's internal security unit with groups of security specialists focused on areas such as threat investigations, offensive engineering, risk management, and product security. Additionally, Yahoo has invested more than $250 million in security initiatives across the company during the current management team's tenure, including creating a "Red Team" and developing the "Bug Bounty" program discussed below.

Below is a list of key product-related initiatives designed to help protect users and supplement Yahoo's broader information security controls and processes:

- Yahoo has restructured the user login history page in the Member Center, enabling users (1) to view the browsers, apps and devices that have accessed their accounts and (2) to terminate existing browser sessions and revoke remote application accesses. Yahoo also launched a "Global Logout" feature in its Member Center that enables users to terminate open sessions that unauthorized parties potentially could access.
- Yahoo has consolidated its registration and login systems into a hardened platform for Yahoo.com web properties and mobile applications, enabling Yahoo to centralize the measurement of suspicious activity to support detection of anomalies and security threats.
- With respect to user password protection, Yahoo uses the bcrypt algorithm, which is a password hashing mechanism that incorporates security features including salting and multiple rounds of computation, to provide advanced protection against password cracking.
- Yahoo continues to enhance its authentication mechanisms, such as by using OAuth (requiring users to opt in to simple, password-based third-party authentication) and leveraging fingerprint-based authentication on certain smartphones.

- Yahoo offers users Yahoo Account Key, an authentication mechanism that eliminates the need to use a password on Yahoo altogether.
- Yahoo applies machine learning artificial intelligence techniques to help detect and prevent fraudulent account access through the company's login interfaces.
- Yahoo has hardened its internal systems including the programmatic interfaces used by the company's software to retrieve user account data.

4. What steps has Yahoo! taken to restore the integrity and enhance the security of its systems in the wake of these incidents?

Yahoo is committed to enhancing the security of the company's infrastructure and products. As the threat landscape evolves, Yahoo continually adapts and modifies the specific measures used to protect and mitigate risk to user data. Even before the relevant incidents were publicly disclosed, Yahoo prioritized resources and accelerated efforts to further enhance its information security posture. In the wake of the incidents, these matters have received and continue to receive significant attention from executives in the company, including near-daily working sessions with the CEO, a security-focused presentation by Yahoo's Chief Information Security Officer at the company's all-hands meeting each week, and focusing engineering personnel on improving the security of the company's products and systems.

In response to the security incidents described in Yahoo's September 22, 2016 and December 14, 2016 disclosures, Yahoo supplemented its own security talent with two leading forensic firms – Stroz Friedberg and Mandiant – to investigate the data security incidents. Investigations to date have found no evidence that the actors believed to be responsible for the relevant incidents are currently in the company's network.

Yahoo continues to take extensive measures, both technical and organizational, to protect its systems. Below are some highlights of Yahoo's investments and improvements focused on talent, processes and security for company systems, users and products:

- Comprehensive Information Security Program: Yahoo has been working to enhance the company's information security program, including its policies, standards and controls. As part of this process, Yahoo focuses its information security program on the NIST Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework"), a globally-recognized, risk-based methodology for organizing and communicating security requirements and managing and mitigating cybersecurity risk. The NIST Cybersecurity Framework revolves around five continuous functions: identify, protect, detect, respond and recover. In addition, Yahoo is working to incorporate within its information security program the most recent version of NIST's Security and Privacy Controls for Federal Information Systems and Organization (NIST Special Publication 800-53), a catalogue of detailed and customizable controls that complement the core NIST Cybersecurity Framework.

In addition to the NIST Cybersecurity Framework, Yahoo has adopted additional security procedures and controls as part of its multi-layered approach to systems and user security, including:

- "Attacker-Centric" Approach: Yahoo organizes its information security program informed by the attacker lifecycle (also known as the "kill chain"). The attacker lifecycle is the set of actions an attacker takes to penetrate company systems to eventually access the systems that have been targeted. By taking into account how attacks work in practice, Yahoo is able to prioritize and focus its security investments. Further, Yahoo staffed a "Red Team," one that adopts the tools and tactics used by adversaries, to assess and help improve the company's defenses and incident response capabilities.

- Organizational Security Measures: Yahoo continues to grow and reinforce its information security program by hiring personnel with experience in risk management, computer science and cybersecurity risk and remediation measures. For example, in recent months, Yahoo has formalized the role of and hired a functional leader for risk management whose chief mandate is to mature Yahoo's formal information security risk management program. In addition, even prior to the data security incidents, Yahoo created an eCrimes team that works with law enforcement to identify and apprehend criminals in the U.S. and abroad, and currently continues to grow its "Red Team," which is focused on identifying vulnerabilities, evaluating Yahoo's security posture and controls, and reporting issues to executive management as appropriate. In addition to its internal vulnerability identification efforts, Yahoo has instituted a formal "Bug Bounty" program, through which Yahoo pays security researchers who report often complex vulnerabilities to the company. Yahoo has spent over $2 million in connection with its Bug Bounty program since the program's inception in 2013 and over 2,600 security researchers around the world have participated in the program to date.

- Reducing Exposure of Sensitive Data: Yahoo has taken steps to mitigate the harm that could result from unauthorized or unlawful access to user data. For example, Yahoo has implemented a process that encrypts the type of files believed to have been affected by the relevant security incidents to help protect user data from unauthorized access. Additionally, in 2014, Yahoo implemented systems to encrypt data in transit between data centers.

- Access Controls and System Hardening: Yahoo has strengthened its access control mechanisms and hardened its systems to reduce the potential attack surface of its environment. For example, Yahoo has reduced the number of systems, services, and personnel that may access the Yahoo systems found to have been affected by the relevant security incidents. Additionally, Yahoo has implemented an initiative that requires two-factor authentication to access relevant production hosts.

- Incident Detection and Monitoring Capabilities: Yahoo continues to prioritize and enhance the company's incident detection, logging, monitoring and response

capabilities on the network, individual host, and product levels to help improve Yahoo's ability to detect and prevent compromises and sophisticated attacks. These capabilities enhance Yahoo's ability to monitor multiple layers of the company's systems and products and to better correlate behaviors across the company's network.

- Advanced Cyber-Threats Team: Yahoo's growing Advanced Cyber-Threats Team and Advanced Persistent Threat ("APT") program aim to track, detect and mitigate threats against Yahoo users posed by advanced adversaries, including state-sponsored actors. Yahoo is implementing systems that will enhance the tracking and management of APT indicators and campaigns, and improve Yahoo's ability to detect and defend against sophisticated threats, including targeted nation-state attacks.

5. In addition to answering these questions, please provide a detailed timeline of these incidents, including Yahoo!'s initial discovery of a potential compromise of its user information, forensic investigation and subsequent security efforts, notifications to law enforcement agencies, as well as any notification to affected consumers.

As previously noted, the information set forth below relates specifically to the company's disclosures on September 22, 2016 and December 14, 2016. As indicated in the Form 10-Q filed with the Securities and Exchange Commission on November 9, 2016, an Independent Committee of the Board of Directors has investigated the company's contemporaneous knowledge, handling and notifications to users regarding the unauthorized access in question. The Independent Committee will provide you with additional information from their investigation relating to contemporaneous knowledge and remediation.

2013 Incident

With respect to the 2013 Incident, in November 2016, law enforcement provided Yahoo with data files that a third party claimed was Yahoo user data. Yahoo analyzed this data with the assistance of outside forensic experts and found that it appeared to be Yahoo user data. Based on further analysis of this data by the forensic experts, Yahoo believes an unauthorized third party, in August 2013, stole data from Yahoo's systems associated with over one billion user accounts. The company has not been able to identify the intrusion associated with this theft. Yahoo believes this incident is likely distinct from the incident the company disclosed on September 22, 2016.

On December 14, 2016, Yahoo began notifying potentially affected users, regulators and other stakeholders, including this Committee, about this issue.

2014 Incident

On September 22, 2016, Yahoo disclosed the 2014 Incident. Following the September 22, 2016, disclosure, the company, with the assistance of outside forensic experts, continued to investigate the 2014 Incident and related matters. The company has also been actively working with U.S. law enforcement authorities on this matter.

As indicated above, an Independent Committee of the Board of Directors of Yahoo, advised by independent counsel and a forensic expert, has investigated the 2014 Incident and related matters, including knowledge of the 2014 Incident within the company in 2014 and thereafter. The Board's Independent Committee will be providing a briefing to the Committee on the findings of these investigations.

Cookie Forging Activity

As indicated above, Yahoo disclosed in November and December 2016 that its outside forensic experts had been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the investigation, Yahoo and its outside forensic experts identified user accounts for which they believe forged cookies were taken or used in 2015 and 2016. As indicated above, Yahoo has connected some of this cookie forging activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016. Yahoo began notifying potentially affected users about this issue on December 14, 2016 and, on February 15, 2017, Yahoo began notifying an additional set of users identified based on the outside forensic experts' ongoing investigation into the cookie forging activity.

Cc: The Honorable Bill Nelson, Ranking Member

The Honorable Richard Blumenthal, Ranking Member
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security