Response to Written Questions Submitted by Honorable Jerry Moran to John Flynn

Question 1. What separates a good faith researcher from a malicious actor? What's to stop a criminal from posing as a researcher? How can companies or vendors tell the difference?

Response. A good faith researcher investigates and discloses vulnerabilities in an ethical manner consistent with the prescribed terms of the bug bounty program. Good faith researchers are generally cooperative throughout the bounty process and willing to abide by the program's rules. Although it may not always be apparent what someone's intentions are or whether a criminal actor is posing as a white hat researcher, certain conduct should raise a red flag. Anyone who in bad faith strays beyond the bounds of the bug bounty program by engaging in behavior such as maliciously compromising user data, making threats, or making extortionate demands should not be considered a good faith researcher.

Question 2. What is the role of bug bounty programs when faced with extortion attempts?

Response. Bug bounty programs are designed for good faith researchers, not extortionists.

Question 3. As you have acknowledged, the hackers involved in the 2016 breach of your company did obtain data of your users. As it relates to Uber's specific bug bounty program, how often is data actually obtained by the hacker that is disclosing a vulnerability to your company? Was the sheer number of exposed and obtained records in the 2016 case unusual compared to other vulnerability disclosure cases your company had witnessed through the bug bounty program?

Response. Most often researchers will use test accounts or access their own data when researching vulnerabilities. If the researcher comes in contact with user data while acting in good faith, the access should be limited to the minimum amount needed to identify and report the vulnerability. We agree that the 2016 incident was unusual compared to other vulnerability disclosure cases witnessed by Uber in terms of sheer number of records.

Question 4. HackerOne's 2018 Hacker Report and a 2016 study conducted by the National Telecommunications and Information Administration (NTIA) both indicated that profit is a relatively limited motivation among hackers participating in coordinated vulnerability disclosure programs. Given the panel's experience with professionals in this field, could you please further describe the predominant motivators.

Response. Historically, before there were bounty programs, researchers would report vulnerabilities as a way to build their reputation in the security community and among their peers. Even today this is the biggest motivator and can open doors for researchers, such as being offered jobs to work for the companies whose vulnerabilities they uncovered.

Question 5. Would you agree that it is absolutely critical for companies to administer any vulnerability disclosure program responsibly based on sound principles (such as those included in DOJ's 2017 guidelines) as it has obvious impacts on industry-wide use of these types of programs that are proven to protect consumers?

Response. Yes. Bug bounty programs are critical for many large companies to detect security issues, and the programs should be designed and managed responsibly so that they can continue to be an important security tool. The DOJ's 2017 framework is a good starting point. It is not prescriptive, but rather outlines a process that companies considering bug bounty programs can follow to clearly define for researchers what the company considers to be authorized vulnerability disclosure and discovery conduct.

Question 6. Did Uber have a pre-determined maximum bounty amount for its bug bounty program? If so, what was the maximum amount?

Response. Uber's Bug Bounty program at HackerOne has a published maximum payment of $10,000, see https://hackerone.com/uber , but the actual amount of any payment under the program is up to Uber in its sole discretion, see https://www.uber.com/legal/other/bug-bounty-program-terms/ ("Bounty payouts, if any, will be determined by Uber in its sole discretion.").

Question 7. Mr. Mickos's testimony stated that the Computer Fraud and Abuse Act is in need of modernization to prevent liability of hackers acting in good faith in identifying vulnerabilities to protect consumers. Do you have any specific recommendations related to modernizing the law?

Response. Other panel participants are closer to these issues, but we at Uber understand that those speaking on behalf of good faith security researchers would like to see more clarity that when conduct complies with the terms of a bug bounty program, it is not "unauthorized" access under the Computer Fraud and Abuse Act.

Question 8. Following an inquiry that I sent along with Chairman Thune and our colleagues from Senate Finance Committee, Uber responded with a letter on December 11, 2017, describing the 2016 breach and the ensuing actions taken by the company. The letter described the payment of $100,000 to the two individual hackers responsible for the breach and stated, "It thereafter engaged in further communications with the two individuals using their real identities, including having them sign assurances that the data was destroyed." For the sake of clarity, was the $100,000 paid to the two individuals prior to their real identities being known?

Response. As I explained in my written testimony, I was not part of the "attribution" team—the team that determined the two individuals' real identities. I was aware that the process of paying them was part of the process of determining their identities, but I am not sure if their identities were confirmed prior to or after the moment the payment was made.

Question 9. Please describe to the greatest extent possible the "assurances" that were made to Uber's "attribution team" that the stolen data had been eliminated. Were signed documents the sole source of assurance?

Response. It is my understanding that the attribution team obtained various sources of information about the destruction of the data, in addition to the signed documents and in person meetings.

Question 10. Please describe the measures Uber has taken to confirm these assurances and monitor the affected accounts for additional fraud protection.

Response. We have seen no evidence of fraud or misuse tied to this incident. That being said, we have identified the 57 million affected accounts in our systems, and have tagged them for a heightened level of fraud protection. Specifically, we have created new fraud "rules" that will surface any unusual activity on the accounts going forward. Uber already looks at many signals like location or device ID, in addition to email address and password, to authorize log-ins to Uber user accounts. Additionally, we automatically send users a second factor authentication request such an SMS or email if we detect a high-risk login attempt.