ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

Statement of **Justin Brookman**
Director, Privacy and Technology Policy
Consumers Union

Before the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers

February 6, 2018

On behalf of Consumers Union, I want to thank you for the opportunity to testify today. We appreciate the leadership of Chairman Moran and Ranking Member Blumenthal in holding today's hearing to explore the still-developing field of bug bounty programs, and how they can best be implemented to promote data security for American consumers.

I appear here today on behalf of Consumers Union, the advocacy division of Consumer Reports, an independent, nonprofit organization that works side by side with consumers to create a fairer, safer, and healthier world.[1]

Consumers Union is a strong proponent of bug bounty programs, and believes that they play a crucial role in a data security ecosystem that has failed consumers far too often. Used properly, bug bounty programs enable companies to learn of breaches and vulnerabilities, in service to the larger goals of protecting consumer data and alerting consumers to threats as warranted and/or required by law. In the case of the 2016 Uber security incident, we believe the company should have disclosed the event earlier, not only because a hacker had accessed sensitive data, but because it appears credentials to that data had been publicly accessible for some time. This incident illustrates the continuing need for Congress to pass legislation providing stronger incentives for companies to deploy reasonable safeguards for personal data.

[1] As the world's largest independent product-testing organization, Consumer Reports uses its more than 50 labs, auto test center, and survey research center to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

I. The Poor State of Modern Data Security and the Importance of Bug Bounty Programs

As this Committee well knows, the story of data security in recent years is not a pretty one. Massive data breaches have become commonplace, as companies accumulate vast troves of valuable consumer data but frequently fail to put adequate systems in place to protect it. The Target data breach of 2013 compromised the information of an estimated 110 million people, including the payment card information of about 40 million consumers.[2] Hackers obtained the data of about 80 million people in the Anthem data breach of 2015.[3] And last year, criminals took advantage of well-known vulnerabilities in software used by Equifax to access the Social Security numbers of over 145 million people.[4] Targeted companies often have the opportunity to head off a breach but neglect to take action. For example, the software vulnerabilities that made Equifax a ripe target for attackers had been public for months, but Equifax failed to address them before the breach.[5]

Bug bounty programs represent a novel and innovative approach to identifying vulnerabilities before they can be taken advantage of by malicious actors. These programs incentivize a diverse third-party ecosystem to probe systems for potential failures. They also provide an alternative to sale of exploits on the black market where they can fetch several hundred thousand dollars — or more.[6] By offering to pay for information directly, companies can offer white- and grey-hat hackers a legal way to monetize their skills, with a far better outcome for companies and consumers. The rapid rise of these programs is evidence of their success. In 2016, Google paid out over $3 million under its bug bounty program for vulnerabilities in products such as Android and Chrome.[7] Last year it partnered with HackerOne to expand the program to cover popular third-party apps in its Google Play Store.[8]

Consumers Union strongly supports the development of bug bounty programs, not just by large tech companies, but for any company that stores sensitive consumer data that could lead to

---

[2] Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. Times, (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html.
[3] Brendan Pierson, *Anthem to Pay Record $115 Million to Settle U.S. Lawsuits over Data Breach*, Reuters (Jun. 23, 2017), https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML.
[4] *Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident*, Equifax.com (Oct. 2, 2017), https://www.equifaxsecurity2017.com/2017/10/02/equifax-announces-cybersecurity-firm-concluded-forensic-investigation-cybersecurity-incident/.
[5] Lily Hay Newman, *Equifax Officially Has No Excuse*, Wired (Sep. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.
[6] Kif Leswig, *Here's what Apple thinks about the black market for $1 million iPhone hacks*, Business Insider, (Jul. 4, 2016), http://www.businessinsider.com/apple-addresses-black-market-for-software-vulnerabilities-2016-6
[7] Taylor Hatmaker, *Google's bug bounty program pays out $3 million, mostly for Android and Chrome exploits*, TechCrunch, (Jan. 31, 2017), https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/.
[8] Liam Tung, *Android Security: Google will pay $1000 for holes in these top apps*, ZDNet, (Oct. 20, 2017), http://www.zdnet.com/article/android-security-google-will-pay-1000-for-holes-in-these-top-apps/.

identity theft, harm, or embarrassment if exposed. In fact, bug bounty programs are identified as an indicator of good data security in the Digital Standard — an open source effort led by Consumer Reports to articulate best practices for privacy, security, ownership, and governance in an increasingly connected world.[9] We launched the Digital Standard with our partners Ranking Digital Rights, Disconnect, and the Cyber Independent Testing Lab in March of last year as part of a strategic shift to start evaluating products for these values as part of our core reviews and ratings service.[10] In addition to highlighting the value of bug bounty programs, the Digital Standard defines as best practices "disclos[ing] the timeframe in which it will review reports of vulnerabilities" and — notable for this hearing — "commit[ting] not to pursue legal action against security researchers."[11]

II. "John Doughs" and the Uber Bug Bounty Program

Although open source software development has always depended on external support to identify errors and weaknesses in code, formal bug bounty programs within major technology companies are still a relatively new phenomenon. As such, it is understandable that expectations, norms, and best practices are still developing in this area.

In 2016, a hacker calling himself "John Doughs" emailed Uber's chief security officer Joe Sullivan that he had discovered a "major vulnerability" in Uber's systems.[12] In subsequent conversations with the hacker, Uber discovered that company engineers had posted credentials to Uber's servers on the code management portal GitHub, and that Doughs had used the credentials to access information about Uber's 57 million user and driver accounts, including sensitive data such as driver's license numbers. Although Uber told Doughs that its maximum bug bounty payout was $10,000, the hacker insisted that he expected "six digits" for his information. Eventually, Uber decided to pay Doughs $100,000, and required him to agree to delete the compromised data.

In general, we believe it is counterproductive to report participants in bug bounty programs to law enforcement absent a strong indication of malicious intent. We are not convinced there is anything wrong *per se* with a hacker asking for more money than is originally offered for information on a vulnerability. A hacker may reasonably believe that the value of the information and the time invested in uncovering it merit a higher payment. In the past, others have criticized Uber's bug bounty program for failing to provide reasonable payments for identifying exploitable

---

[9] The Digital Standard, https://www.thedigitalstandard.org/.
[10] Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security, CONSUMER REPORTS, (Mar. 6, 2017), https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/
[11] The Digital Standard, Data Security, Vulnerability disclosure program, https://www.thedigitalstandard.org/the-standard.
[12] Nicole Perlroth and Mike Isaac, *Inside Uber's $100,000 Payment to a Hacker, and the Fallout*, N.Y. TIMES, (Jan. 12, 2018), https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html.

holes in their code.[13] At some point, a request for more money may convey an implicit — or explicit — threat to sell the exploit or compromised data elsewhere if the demands are not met. However, from the publicly reported facts, it is not clear that that happened in this case. In any event, Uber had invited persons such as Doughs to look for precisely the type of vulnerabilities that he eventually found. If security researchers have to worry that looking for bugs in code will lead to criminal referral, the efficacy of bug bounty programs will dramatically decrease.

Nevertheless, Uber had an ethical — and legal — obligation to be more forthcoming with its users after it was made aware of its security lapse. Forty-eight states — as well as the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands have laws mandating disclosure to consumers when their personal information is jeopardized in a security breach.[14] Drivers' license information — which was compromised in this incident — is typically included within such laws. While breach notification triggers vary significantly among the states, it seems quite likely that at least some state laws mandated disclosure to Uber drivers about the incident. For example, California law requires breach notification when "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." While many other states only require notification upon a determination that no harm was likely to have occurred, it is not clear how Uber could have reasonably come to this conclusion. Even if Uber felt it could trust that John Doughs had not sold or copied the data, Uber knew that credentials to its servers had been publicly accessible in Github and could have been used by others to access sensitive personal information.[15] Uber is in constant communication with its drivers and could easily have told them about the potential exposure of their information; instead they decided to say nothing.

State data breach notification laws were first passed starting in 2002, and were clearly not written with bug bounty programs in mind. Notification laws and bug bounty programs both play an important role in protecting consumers, but there is a potential conflict between the two that needs to be reconciled. Indeed, notifying consumers of breaches created by ethical hacking pursuant to bug bounty programs could unnecessarily alarm consumers without providing any clear benefit.[16] Lawmakers seeking to update these protections must be extremely careful to

---

[13] Gregory Perry, *How I Got Paid $0 From the Uber Security Bug Bounty*, MEDIUM, (Dec. 24, 2017), https://medium.com/bread-and-circuses/how-i-got-paid-0-from-the-uber-security-bug-bounty-aa9646aa103f

[14] Security Breach Notification Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES, (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[15] Jeremy Kahn, *Uber Hack Shows Vulnerability of Software Code-Sharing Services*, BLOOMBERG, (Nov. 22, 2017), https://www.bloomberg.com/news/articles/2017-11-22/uber-hack-shows-vulnerability-of-software-code-sharing-services.. This was not the first time Uber credentials posted to GitHub led to a data security incident; in 2014, credentials posted in a publicly available GitHub repository compromised the data of 50,000 users. *Id.*

[16] Similarly, security researchers have called for modifications to the Wassenaar anti-proliferation agreement to allow for cross-border communications about security vulnerabilities and the effective management of bug bounty programs. *See* James Sanders, *How the Wassenaar Arrangement threatens*

balance the security benefits provided by external hacking with the right of consumers to know when their information is truly at risk, perhaps by developing general standards to govern the legitimate use of these programs. In any event, Uber was not entitled to simply decide not to follow consumer protection (and other) laws it believed to be onerous or unnecessary. Uber previously took over six months to announce a different data breach in 2015, making the delay in announcing the 2016 breach all the more difficult to justify.[17] Further, if in fact a condition of the payment to Doughs was that he could not disclose the incident — even after the vulnerability had been remedied so no one could exploit it — then the lack of transparency from Uber is still more concerning.[18]

III. New Laws are Needed to Provide for Better Security Incentives

Bug bounty programs should continue to play an important role in safeguarding consumers personal information. And Consumer Reports is committed to providing more information to the marketplace about which companies perform best under the Digital Standard, including which companies have the best security practices.

However, due to a misalignment of incentives, most companies today do not adequately invest in cybersecurity. Many breaches are not detected or publicly disclosed. The likelihood of law enforcement under the current regulatory scheme is low. The potential profits from using consumer data far outweigh any penalties that can be assessed for violations, incentivizing carelessness and misuse. And companies that experience a data breach bear only a portion of the cost — much of that instead is laid on consumers. As such, we need a much stronger data security law in the United States.

Americans lost an estimated $16 billion to identity theft in 2016, up almost $1 billion from the year prior.[19] Department of Justice data reveals that about 7% of Americans over the age of 16

---

responsible vulnerability disclosures, TechRepublic, (Jul. 7, 2015), https://www.techrepublic.com/article/how-the-wassenaar-arrangement-threatens-responsible-security-vulnerability-disclosures/.

[17] Dave Lewis, *Uber Suffers Data Breach Affecting 50,000*, Forbes, (Feb. 28, 2015), https://www.forbes.com/sites/davelewis/2015/02/28/uber-suffers-data-breach-affecting-50000/#5e59102c2db1.

[18] Mike Isaac, Katie Brenner, and Sheera Frankel, *Uber Hid 2016 Data Breach, Paying Hackers to Delete Stolen Data*, N.Y. Times, (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html. Even today, Uber and HackerOne, despite publishing statistics about the bug bounty program, appear to be omitting inclusion of this incident. The bounty program's webpage states that its top bounties range between $4,400 and $20,000, despite reports that John Doughs was paid over $100,000 for information about this security vulnerability. *See Uber: Bug Bounty Program*, Uber, https://hackerone.com/uber. This is despite the site denoting "AWS credential exposure resulting in access to driver documents" as an example of in-scope vulnerability class examples — precisely the vulnerability exposed by Doughs.

[19] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Javelin (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraudhits-record-high-154-million-us-victims-2016-16-percent-according-new.

experienced identity theft in 2014.[20] About 9% spent a month or more repairing their accounts or credit histories.[21] Tax identity theft—when identity thieves use compromised social security numbers to file taxes and collect the refund—is a significant concern as well. In fiscal year 2016, the Internal Revenue Service discovered fraudulent returns filed for nearly 1 million people, totaling $6.5 billion.[22] And because consumers often cannot reliably attribute these losses to particular companies, those companies typically can't be held responsible in court for consumers' losses.

Congress needs to act to update consumer protections to reflect the extremely real threats poses to consumers by poor security practices.

First, lawmakers should give the Federal Trade Commission (FTC)[23] stronger resources and tools to protect consumers. The FTC has a long, bipartisan history of responding to an ever-changing array of threats on behalf of the American people. However, the agency does not have sufficient resources to police the marketplace as it should, and there are gaps in its authority to address privacy and data security lapses in various sectors. For example, it currently lacks the authority to take action against nonprofit entities and "common carriers."[24] Moreover, when it does bring a case against a bad actor, it typically lacks the authority to obtain civil penalties to deter potential wrongdoers from similar behavior. As such, deceptive or unfair business practices can be rationalized by companies as a (fairly low) cost of doing business.

Second, Congress should pass legislation requiring companies that have access to sensitive personal information to use reasonable security to safeguard it. Despite the FTC's long-standing use of the FTC Act to address data security lapses, some companies continue to challenge it.[25] The FTC to date has brought over 60 cases challenging shoddy data security practices, but given the uncertainties in application, challenges in attributing harm to specific incidents, and the lack of penalties, the market has yet to internalize the risks posed to consumers by potential data breaches.

---

[20] U.S. Dep't of Justice, Victims of Identity Theft, 2014 1 (Sep. 2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[21] *Id.* at 10.
[22] Written Testimony of John A. Koskinen Before the Senate Finance Committee on the 2017 Filing Season and IRS Operations, INTERNAL REVENUE SERV. (Apr. 6, 2017), https://www.irs.gov/newsroom/writtentestimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operationsapril-6-2017.
[23] From August 2015 to August 2017, I served as Policy Director of the FTC's Office of Technology, Research, and Investigation.
[24] Oral Statement of Commissioner Terrell McSweeny before the House Judiciary Committee, (Nov. 21, 2017), https://www.ftc.gov/system/files/documents/public_statements/1268963/mcsweeny_oral_testimony_to_us_house_of_representatives_committee_on_the_judiciary_11-1-17_.pdf.
[25] *E.g.*, Mallory Locklear, *FTC lawsuit over D-Link's lax router security just took a big hit*, ENGADGET, (Sep. 21, 2017), https://www.engadget.com/2017/09/21/ftc-lawsuit-d-link-lax-router-security-took-hit/.

Finally, while the vast majority of American citizens are protected by state data breach notification laws today, a federal standard has the potential to strengthen these requirements and impose stronger penalties. However, the goal of any federal breach notification law must be to strengthen consumer protections, not weaken the already inadequate incentives in place today. As a result, any such bill should include the resources and stronger authority for the FTC discussed above. Further, it must not broadly preempt state breach and security laws that cover information outside the scope of a federal law.

Indeed, states must be allowed and encouraged to continue to innovate to protect their citizens. States have been the leaders in passing and revising data breach notification legislation over the years. At first, these laws primarily covered financial information such as Social Security numbers and credit card account numbers. However, over time, several states have extended these laws to cover new categories of information that, if compromised, pose risks to consumers. For instance, some states have extended breach notification protections to email and photo storage accounts, recognizing that those databases contain incredibly personal information, and could be leveraged for new types of damaging identity theft.[26] States must be allowed to iterate over time to protect their citizens from new and emerging security threats.

Conclusion

Thank you again for the opportunity to testify here today about the challenges of implementing bug bounty programs to best safeguard personal information. We believe that these programs play a vital role in uncovering vulnerabilities in code before they can be exploited by malicious actors. However, in order to incentivize companies to deploy these and other data protection safeguards, Congress must update consumer protection laws for the modern age to account for the unprecedented threats to our personal data. I look forward to answering the Committee's questions.

[26] *E.g.*, *Delaware Amends Its Data Breach Notification Law*, MAYER BROWN, (Aug. 29, 2017), https://www.mayerbrown.com/delaware-amends-its-data-breach-notification-law-08-29-2017/.