hackerone

July 22, 2019

SUBMITTED VIA E-MAIL

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW.
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218, mail stop 9W-11
Washington, DC 20219

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: Advance Notice of Proposed Rulemaking – Enhanced Cyber Risk Management Standards; Federal Reserve Docket No. R-1550, RIN 7100-AE-61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45

Dear Ladies and Gentlemen:

HackerOne Inc. ("HackerOne")[1] submits this letter in response to the request for comment on the Advance Notice of Proposed Rulemaking ("ANPR") referenced above[2] by the Board of Governors of the Federal Reserve System (the "Board"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposition Insurance Corporation ("FDIC") (collectively, the agencies).

Although the comment period for this ANPR closed over two years ago, the agencies have yet to publish a proposed rule and recent developments in the cyber risk management space

[1] HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Goldman Sachs, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center, and over 1,300 other organizations have partnered with HackerOne to resolve over 120,000 vulnerabilities and award over $51 million in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

[2] Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74315 (Oct. 26, 2016).

warrant further comment. In particular, the increased adoption across the federal government and the financial services industry of vulnerability disclosure policies ("VDPs") and bug bounty programs ("BBPs") suggests that these critical pieces of cybersecurity infrastructure should be a part of any forthcoming Enhanced Cyber Risk Management Standards. VDPs and BBPs offer alternatives to prescriptive regulation and are already being integrated as best practices into covered entities' cybersecurity frameworks.

A. **What are VDPs and BBPs?**

A Vulnerability Disclosure Policy, or VDP, is an organization's formalized method for receiving vulnerability submissions from the outside world. This practice is outlined in the Department of Justice's *Framework for a Vulnerability Disclosure Program for Online Systems*[3] and defined in International Organization for Standardization ("ISO") Standard 29147.[4] It is a reactive form of receiving bugs: we accept the work of the security community and will do our best to resolve issues found. In other words, it is the digital equivalent of "if you see something, say something." It is intended to give anyone—ethical hackers (aka "researchers" or "finders"), or anyone who stumbles across something amiss—clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.

On the other hand, a Bug Bounty Program, or BBP, is an organization's bounty-driven rewards program inviting any hacker (public BBP) or a select group of hackers (private BBP) to find exploits and vulnerabilities in its systems. It is a proactive challenge to look for bugs: we actively encourage the security community to target the assets we choose, to help improve our security. BBPs involve payment to bug hunters.

A well-established VDP coupled with a BBP implemented in a progressive fashion are commonly seen as the most effective and inexpensive way to identify and ultimately remediate cyber vulnerabilities in live systems, assets, and products. Private BBPs often work best when a company is still building its cybersecurity infrastructure, while public BBPs require a certain degree of cybersecurity maturity and generally should only be used when they can be responsibly and properly managed.

B. **Recent Developments Warrant Further Comment on the ANPR.**

Data breaches and other instances of cyberattacks are on the rise. For example, fraud incidents in the financial services sector, both online and offline, increased by more than 130% in 2017, resulting in significant monetary and reputational losses for financial institutions.[5] Even with regular penetration testing, companies are looking for more diverse security testers and a more holistic approach to take a critical look at their systems to ensure security. Since the ANPR

[3] *A Framework for a Vulnerability Disclosure Program for Online Systems* (v1.0), DOJ (July 2017), *available at* https://www.justice.gov/criminal-ccips/page/file/983996/download.

[4] ISO/IEC 29147:2018 ("Information technology -- Security techniques -- Vulnerability disclosure"). The standard details the methods a vendor should use to address issues related to vulnerability disclosure.

[5] *Top Financial Services Issues of 2018*, PwC (Dec. 2017), *available at* https://www.pwc.com/us/en/financial-services/research-institute/assets/pwc-fsi-top-issues-2018.pdf.

was published in 2016, the federal government and the financial services industry are currently racing in parallel to put in place VDP and BBP best practices to detect and mitigate cyber vulnerabilities.

Last month, the National Institute of Standards and Technology ("NIST") published for comment a cybersecurity white paper on "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)."[6] In it, NIST recommends a set of core, high-level SSDF practices to be added to each software development life cycle implementation. Of note, it recommends the identification and confirmation of vulnerabilities on an ongoing basis through the establishment of vulnerability response programs.[7] This white paper follows a 2016 NIST report to the White House Office of Science and Technology Policy on reducing software vulnerabilities.[8] In that report, NIST acknowledged that "[c]ybersecurity has not kept pace" with vulnerabilities, and that change is needed to "stop[] them before they occur, by finding them before they are exploited or by reducing their impact."[9] NIST also recently updated its Cybersecurity Framework to include a core element ensuring effective response to findings of vulnerabilities—i.e., "Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and *external* sources (e.g. internal testing, security bulletins, or *security researchers*)."[10]

Separately, the Department of Defense ("DoD") has expanded its successful "Hack the Pentagon" program, where a pre-vetted group of hackers assists DoD from the early stages of application development in rooting out vulnerabilities,[11] and the Department of Homeland Security is in the process of establishing a bug bounty program of its own.[12] Congress also is moving forward with similar programs for the Department of State. The "Hack Your State Department Act" would require the Secretary of State to "design and establish a Vulnerability Disclosure Process (VDP) to improve Department of State cybersecurity and a bug bounty

[6] *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*, NIST (draft June 11, 2019), *available at* https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft. The comment period is open until August 5, 2019.

[7] *Id.* at 15 (RV.1).

[8] Paul E. Black, et. al, *Dramatically Reducing Software Vulnerabilities* (NISTIR 8151), NIST (Nov. 2016), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf.

[9] *Id.* at 2.

[10] *Framework for Improving Critical Infrastructure Cybersecurity* (v1.1), NIST, at 42 (Apr. 16, 2018) (emphasis added), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. *See also* Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (revision 2), NIST, at 25 (Dec. 2018) ("Make the transition to *ongoing authorization* and use *continuous monitoring* approaches to reduce the cost and increase the efficiency of security and privacy programs.") (emphasis in original), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[11] *See* Aaron Boyd, *DOD Invests $34 Million in Hack the Pentagon Expansion*, NEXTGOV (Oct. 24, 2018), https://www.nextgov.com/cybersecurity/2018/10/dod-invests-34-million-hack-pentagon-expansion/152267/.

[12] The National Telecommunications and Information Administration ("NTIA"), the Federal Trade Commission ("FTC"), and the Food and Drug Administration ("FDA") also all have issued cybersecurity recommendations.

program to identify and report vulnerabilities of internet-facing information technology of the Department of State."[13]

The financial services sector, moreover, has embraced VDPs and BBPs and have incorporated them into their cybersecurity frameworks (even absent any regulatory mandates). For example, Goldman Sachs partnered with HackerOne to not only create a clear avenue for researchers to submit vulnerabilities on their public facing assets, but also show a public commitment to security.[14] Of note, Goldman Sachs launched a private bug bounty program on HackerOne's platform in November 2017, and transitioned to a public bug bounty program in June 2019. Other financial services companies that have publicly engaged with HackerOne include: PayPal (an online payments system), LocalTapiola (an insurance company), LendingClub (a peer-to-peer lending company), and Coinbase (a digital currency exchange).[15]

C. **VDPs and BBPs Should be an Explicit Part of Any Forthcoming Enhanced Cyber Risk Management Standards.**

As the agencies continue to move forward with their rulemaking on Enhanced Cyber Risk Management Standards, they should incorporate the role that VDPs and private BBPs play in covered entities' effective cybersecurity governance programs.[16] Such programs should be seen as baseline activities, whereas public BBPs require a higher degree of risk management maturity.

First, there is value in hacker-powered security—i.e., any cybersecurity-enhancing services and automations that are partially or wholly produced by independently operating security experts outside of the company or organization. At scale, hacker-powered security has the opportunity to ultimately detect every hole, every weakness, and every security vulnerability in a system or product built by humans. While penetration testing is limited in time and scope, hacker-powered security is continuous and wider in scope. As software dependence and building grows and data volumes swell to new highs, working with a recognized community dedicated to uncovering new holes in both old and new software allows companies to continue to move at the pace of innovation while knowing their systems are constantly being checked.

Second, covered entities must be prepared to continually identify and respond to cybersecurity vulnerabilities in their systems. And although many organizations do not have sufficient internal resources to monitor for these vulnerabilities,[17] they can establish VDPs to

[13] H.R. 328 (116th Congress; passed the House on Jan. 22, 2019). A companion bill, S. 1808, was introduced in the Senate on June 12, 2019.

[14] *Goldman Sachs*, HACKERONE, https://hackerone.com/goldmansachs (last visited July 19, 2019).

[15] HackerOne also contracts privately with a number of other financial services companies.

[16] Question 16 in the ANPR specifically asked, "Besides the approach outlined in the ANPR, what other approaches could ensure that entities are effectively identifying, monitoring, measuring, managing, and reporting on cyber risk?" 81 Fed. Reg. at 74322.

[17] A recent jobs report estimated that there will be 3.5 million cybersecurity job openings by 2021. *Cybersecurity Jobs Report*, HERJAVEC GROUP, at 2 (ed. 2018-2021), *available at* https://www.herjavecgroup.com/wp-content/uploads/2018/11/HG-and-CV-Cybersecurity-Jobs-Report-2018.pdf.

allow good Samaritans to report weaknesses that might not otherwise have been uncovered. VDPs give these individuals clear reporting channels and provide some legal liability protection. In establishing a VDP, a covered entity also should have in place proper procedures to pass along vulnerabilities that come to its attention that apply to another entity. Best practices for VDPs can be found in ISO 29147 and 30111.[18]

Generally, there are five key components of a VDP:

- **Promise**: Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities;

- **Scope**: Indicate what properties, products, and vulnerability types are covered;

- **Safe Harbor**: Assures that reporters of good faith will not be unduly penalized;

- **Process**: The process finders use to report vulnerabilities; and

- **Preferences**: A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Finally, BBPs provide for a more dynamic and fluid approach to testing a covered entities' securities beyond penetration testing. While a penetration test is a one-time, automatic or manual test of an entity's security systems, a BBP is a continuous security test that rewards ethical hackers for finding vulnerabilities. Payment is made only when an in-scope vulnerability is found. Most importantly, a properly administered BBP can find vulnerabilities that penetration tests may not be able to uncover.

While the ANPR hints at a covered entities' use of VDPs and BBPs,[19] the recent increase in references to and the use of BBPs and VDPs both in the public and private sectors should suggest to the agencies that explicit reference to these two critical pieces of cybersecurity infrastructure in any forthcoming Enhanced Cyber Risk Management Standards is warranted. Reference to implementation of VDPs and BBPs would emphasize the need for covered entities to continuously monitor and manage their cyber risk.

* * *

[18] ISO/IEC 29147:2018, *supra* note 4; ISO/IEC 30111:2013 ("Information technology -- Security techniques -- Vulnerability handling processes").

[19] *See, e.g.*, 81 Fed. Reg. at 74322 ("Such an evaluation would be required to include the entire security lifecycle, including penetration testing and other vulnerability assessment activities as appropriate based on the size, complexity, scope of operations, and interconnectedness of the covered entity.").

HackerOne thanks the agencies for considering its comments. Should you have any questions, please contact me at deborah@hackerone.com.

Sincerely,

[redacted]

Deborah Chang
Vice President, Business Development and Public Policy
HackerOne

•