United States Senate
WASHINGTON, DC 20510

August 16, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Dear Director Easterly:

On August 15, 2024, National Public Data (NPD) acknowledged it experienced a cyberattack from a third-party bad actor in late December 2023 that reportedly resulted in a breach of personal data.[1] NPD publicly stated that personally identifiable information (PII), including names, email addresses, phone numbers, social security numbers, and mailing addresses were suspected of being obtained.[2] According to a recently-filed class action lawsuit, the unencrypted data was later shared on the dark web in April, and reports also indicate this summer.[3] The suit further alleges that the hacker group USDoD is responsible for the cyberattack.[4] Further, according to recent reports, a hacker known as "Fenice" leaked a version of the stolen NPD data on the dark web.[5] The hacker claimed the data included 2.7 billion "records" of PII, though NPD has not acknowledged the number of users that were impacted.[6] However, according to the lawsuit, USDoD claimed to have records of 2.9 billion "individuals," and sought a purchase price of $3.5 million for the data.[7]

I've previously raised concerns about the need to hold private entities that play a part in protecting our nation's cybersecurity accountable for cyberattacks that compromise Americans' data.[8] In June, I joined bipartisan legislation to help protect American data from malicious

---

[1] National Public Data, Security Incident (Aug. 15, 2024), https://nationalpublicdata.com/Breach.html; Office of Secretary of State, Division of Corporations, State of Florida, Application for Registration of Fictitious Name, Document # G2200004009 (Mar. 29, 2022), https://dos.sunbiz.org/pdf/90692289.pdf (Jerico Pictures, Inc. is doing business as National Public Data.)
[2] *Id*.
[3] Compl., *Hofmann v. Jerico Pictures, Inc.*, Docket No. 0:24-cv-61383-DSL at 2, 4 (S.D. Fla. Aug. 1, 2024), https://www.documentcloud.org/documents/25038487-hoffman-npd-class-action-lawsuit; *see also* Aimee Picchi, *Hackers may have stolen the Social Security numbers of many Americans. Here's what to know*, CBS NEWS (Aug. 15, 2024), https://www.cbsnews.com/news/social-security-number-leak-npd-breach-what-to-know/.
[4] *Hofmann v. Jerico*, *supra* note 3 at 6.
[5] Picchi, *supra* note 3; Lawrence Abrams, *Hackers leak 2.7 billion data records with Social Security numbers*, BLEEPING COMPUTER (Aug. 11, 2024), https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/.
[6] *Id.*; National Public Data, *supra* note 1.
[7] *Hofmann v. Jerico*, *supra* note 3 at 6; *see also* @H4ckManac, TWITTER (Apr. 8, 2024, 4:05 AM), https://x.com/H4ckManac/status/1777246310782902686/photo/1.
[8] Press Release, Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, Grassley, Cortez Masto Work To Protect Americans' Data (June 20, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-

foreign entities by requiring websites and apps to disclose to users if they're subject to the control of China, North Korea, Russia or Iran.[9] Earlier this month, I also sent letters to AT&T and 17 federal agencies regarding the April 2024 cyberattack on AT&T that breached 90 million Americans' data, potentially including federal agencies' communications patterns.[10] As an entity that handles millions of Americans' PII, it is imperative that NPD ensures its data is secure from bad actors.

Accordingly, so Congress may conduct objective and independent oversight concerning the December 2023 NPD cyberattack and subsequent disclosure of personal data, please provide answers to the following no later than August 30, 2024:

1. Has CISA been in contact with NPD? If so, when?

2. Does CISA use NPD to conduct background checks? If so, was CISA impacted by the December 2023 cyberattack? Describe in detail how CISA was impacted, if applicable.

3. Is CISA aware of other federal agencies that use NPD to conduct background checks? If so, provide a list of agencies using NPD and note whether those agencies were affected by the data breach.

4. What steps is CISA taking to work with NPD to secure affected federal agencies and Americans' PII? Provide all records.[11]

Thank you for your prompt review and response. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-0642.

Sincerely,

Charles E. Grassley
Ranking Member
Committee on the Budget

---

cortez-masto-work-to-protect-americans-data; Press Release, Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, Grassley Conducts Sweeping Oversight Of Recent AT&T Hack, Potential National Security Risks (Aug. 5, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-conducts-sweeping-oversight-of-recent-atandt-hack-potential-national-security-implications; *see also* Press Release, Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense (Apr. 8, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-federal-agencies-must-stop-dragging-their-feet-on-bolstering-cybersecurity-defense.

[9] Grassley, Cortez Masto Work To Protect Americans' Data, *supra* note 8.

[10] Grassley Conducts Sweeping Oversight Of Recent AT&T Hack, Potential National Security Risks, *supra* note 8.

[11] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).