

United States Senate
WASHINGTON, DC 20510

August 16, 2024

VIA ELECTRONIC TRANSMISSION

Salvatore Verini, Jr.
President
Jerico Pictures, Inc.
d/b/a National Public Data

Dear Mr. Verini:

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’

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>.

data.⁸ In June, I joined bipartisan legislation to help protect American data from malicious 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. How many records did the third party hackers obtain from NPD? How many individuals were affected by this breach? Provide all records from NPD's internal investigation into this incident.¹¹
2. Provide all communications between and among NPD and federal, state, and local law enforcement relating to breach.
3. Do any federal agencies use NPD for background checks? If so, which ones? Of those:
 - a. Which federal agencies were impacted by the December 2023 cyberattack? Explain how they were impacted.
 - b. Has NPD communicated with all of these entities? If not, why not?
4. Where does NPD store its data? Provide a list of locations where NPD data is stored and NPD's policies and procedures regarding securing the data.
5. Why does NPD store PII? How long is it stored? Please explain.

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-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).

6. Are the reports that the data was unencrypted accurate? If so, why was the data unencrypted? Please explain.
7. Does NPD contract with any federal agencies to access nonpublic databases? If so, list each agency and database.
8. Does NPD sell any of its stored data to other data brokers or foreign countries? If so, what kind of data is stored and what kind of data is sold? List each data broker and foreign country.
9. Was NPD aware of any potential vulnerabilities before the December 2023 cyberattack? If so, what measures did NPD take to secure its data? Provide all records.
10. What specific steps is NPD taking to secure its data from future data breaches and cyberattacks? Provide all records.

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