KRONENBERGER ROSENFELD

FOIA CONFIDENTIAL TREATMENT REQUESTED

August 28, 2024

Tucker A. Akin, Investigative Counsel
For Charles E. Grassley, U.S. Senate Budget Committee
Washington, DC 20510
Tucker_Akin@[redacted]
cc: [redacted]; Josh_Flynn-Brown@[redacted]

VIA EMAIL

RE: 2024-08-16 CEG to Jerico Pictures, Inc. dba National Public Data (NPD); NPD's Confidential and Voluntary Responses to the Senator's Inquiry

Dear Tucker Akin:

Our firm is legal counsel to Jerico Pictures, Inc. dba National Public Data (NPD) in this matter. This letter responds to your August 16, 2024 email, which attached a letter from Senator Charles E. Grassley. Our client respects the Senator's commitment to data privacy and security issues and welcomes this opportunity to voluntarily cooperate and provide certain clarifications. NPD provides the below responses and requests confidential treatment for this information.

Background

For context, NPD has been an established lawful business that primarily processed public data, like numerous other companies, in the United States. Due to recent events, including legal actions/investigations from state, federal, and private parties, NPD, which has been managed by a sole owner, has been forced to file for a petition for bankruptcy.

Despite certain implications, NPD was operating under the confines of existing laws, where regulations about consumer data are still evolving; and despite its efforts, NPD was a victim of a notorious bad actor, a hacker who also hacked the FBI twice along with other government agencies and large companies. This hacker is also a known exaggerator and liar with ulterior motives related to the launch of a separate criminal operation, and many allegations about the NPD security incident have been either outright false or misinterpreted. As just one example, your letter asked about 2.9 billion "individuals" subject to a data breach, which would be impossible e.g., there are far fewer individuals in the United States, and NPD never possessed such a file.

Importantly, after suspecting that there was a limited security incident, NPD immediately reasonably responded, including by contacting separate legal counsel and the FBI and other law enforcement. NPD has been fully cooperative with the FBI and other agency investigations, and the FBI investigation is still ongoing. To clarify any misconceptions from the media, NPD's efforts have been ongoing since December 2023, including through attempts to mitigate harm and then in providing data breach notifications to groups of consumers starting in April 2024 as more information was obtained, even though there is still lacking confirmation about the data and individuals at issue.

Responses to Specific Questions

While NPD is voluntarily providing these responses, NPD objects to the requests to the extent they are: overly broad and oppressive, based on claims that are not supported, and not reasonably relevant to any legitimate inquiry or investigation. NPD also reserves the right to submit additional objections and change any responses as information is obtained and reviewed.

Question 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.

Response: This question relates to an ongoing FBI investigation with Agent Ryan Shafer, which limits NPD's ability to provide all records. NPD has worked with counsel to provide data breach notifications to two groups, one comprised of **109 individuals** and the other comprised of **1,350,684 individuals**.

Question 2. Provide all communications between and among NPD and federal, state, and local law enforcement relating to breach.

Response: This question relates to an ongoing FBI investigation as well as ongoing federal, state, and law enforcement investigations, which limits NPD's ability to provide all communications.

Question 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?

Response: No, none are known.

Question 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.

Response: NPD has stored data in two separate data centers in Florida. NPD has had various policies and procedures regarding data security, including for securing data, which have updated over time and have included a data security policy and other policies, firewall controls, use of encryption, network segregation, third-party IT, use of a secure server (i.e., locked cage in data center), port blocking, software protection, checking logs/server, updating and using secure passwords, monitoring where data is stored, and limiting data processed and access to data.

Question 5. Why does NPD store PII? How long is it stored? Please explain.

Response: NPD stored data in its normal course of business for the length of time necessary for its business or to comply with legal obligations, subject to applicable (or lacking) laws.

Question 6. Are the reports that the data was unencrypted accurate? If so, why was the data unencrypted? Please explain.

Response: There are various reports that are inaccurate. NPD used encryption tools for data. There was also limited data in a development database that was still under construction.

Question 7. Does NPD contract with any federal agencies to access nonpublic databases? If so, list each agency and database.

Response: No, none are known.

Question 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.

Response: No, NPD does not sell data to foreign countries; NPD does not sell non-public or sensitive data to data brokers. To clarify, the database in question was not for sale.

Question 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.

Response: No, NPD was not aware of vulnerabilities. Nonetheless, NPD took various measures to secure data, including as described above. This question relates to an ongoing FBI investigation, which limits NPD's ability to provide all records.

Question 10. What specific steps is NPD taking to secure its data from future data breaches and cyberattacks? Provide all records.

Response: NPD promptly worked with a third-party IT consultant, including to confirm that the hacker's access was terminated and to audit its systems. In addition, NPD has limited the scope of data processed, worked with legal counsel to update its security policies, and implemented additional safeguards. Data security measures are also outlined above for question 4. This question relates to an ongoing FBI investigation, which limits NPD's ability to provide all records.

This letter does not constitute a complete or exhaustive statement of all of NPD's rights, claims, contentions, or legal theories regarding this matter. Nothing stated herein is intended as, nor should it be deemed to constitute, a waiver or relinquishment of any of NPD's rights or remedies, whether legal or equitable, all of which are hereby expressly reserved.

If you have any questions about this matter, you may reach me at [redacted], or at [redacted]

Sincerely,

KRONENBERGER ROSENFELD, LLP

Karl S. Kronenberger
Partner