Report on ITM-Evidence Based Learning

National Public Data Breach (2024)

Academic Year : 2024-25	**Class : TE**
Semester : II	**Date of Submission : 29/03/2025**
CO : CO 311.6	**PO : 2, 4, 8, 10 PSO : 2**
Roll No : 58	**Name: Shweta**

1. Summary

The **2024 National Public Data Breach** was one of the largest cyberattacks in history, affecting **2.9 billion records**. It targeted **National Public Data**, a data broker company specializing in background checks. The breach exposed sensitive personal information, including **Social Security numbers, addresses, and employment history**, leading to numerous lawsuits and the company's eventual bankruptcy. This case study examines how the breach occurred, how it was detected, the legal actions taken, and ethical considerations for preventing such incidents.

2. Introduction

The purpose of this case study is to analyze the **2024 National Public Data Breach**, focusing on the methods used by cybercriminals, the impact on individuals and organizations, and the legal and ethical implications. Data breaches have become a significant concern, particularly for companies handling personal information. This study references reports, cybersecurity analyses, and legal frameworks related to the incident.

3. Findings

How the Crime Happened

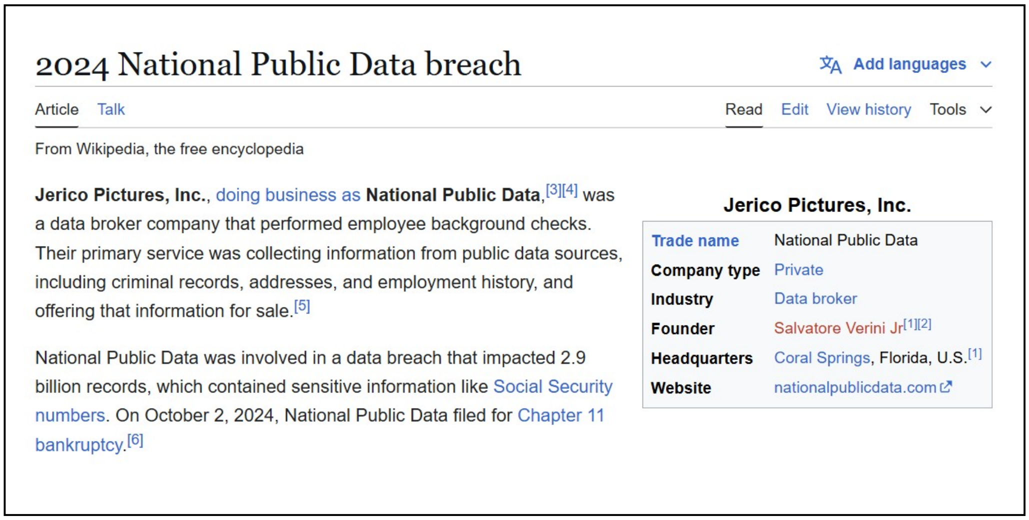
- The breach originated from a **persistent cyberattack** detected in **December 2023**.
- By **April 2024**, hackers successfully **infiltrated the database** through vulnerabilities in the company's security system.

- A hacker using the alias **“USDoD”** allegedly stole the data and listed it on the **dark web** for sale at **$3.5 million**.

How the Crime Was Detected

- **August 16, 2024**: National Public Data confirmed the breach after detecting suspicious activities and reports of stolen data appearing online.
- Multiple **class-action lawsuits** were filed, accusing the company of negligence in protecting sensitive data.
- Investigations revealed that **hacking attempts had been ongoing for months** before the data was fully compromised.

4. News Paper Cutting



2024 National Public Data breach

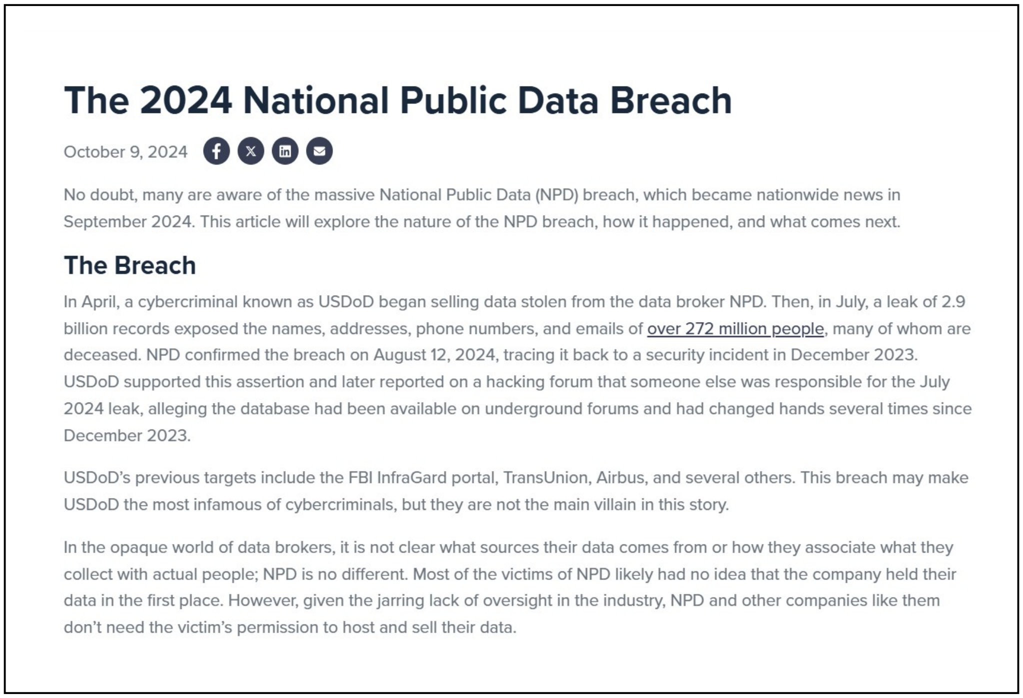
From Wikipedia, the free encyclopedia

Jerico Pictures, Inc., doing business as **National Public Data**,[3][4] was a data broker company that performed employee background checks. Their primary service was collecting information from public data sources, including criminal records, addresses, and employment history, and offering that information for sale.[5]

National Public Data was involved in a data breach that impacted 2.9 billion records, which contained sensitive information like Social Security numbers. On October 2, 2024, National Public Data filed for Chapter 11 bankruptcy.[6]

Jerico Pictures, Inc.

Trade name	National Public Data
Company type	Private
Industry	Data broker
Founder	Salvatore Verini Jr[1][2]
Headquarters	Coral Springs, Florida, U.S.[1]
Website	nationalpublicdata.com



The 2024 National Public Data Breach

October 9, 2024

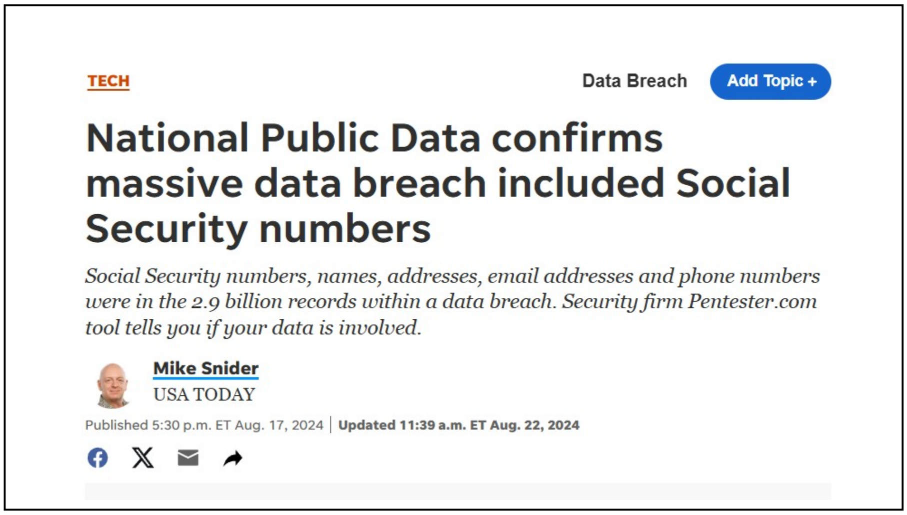
No doubt, many are aware of the massive National Public Data (NPD) breach, which became nationwide news in September 2024. This article will explore the nature of the NPD breach, how it happened, and what comes next.

The Breach

In April, a cybercriminal known as USDoD began selling data stolen from the data broker NPD. Then, in July, a leak of 2.9 billion records exposed the names, addresses, phone numbers, and emails of over 272 million people, many of whom are deceased. NPD confirmed the breach on August 12, 2024, tracing it back to a security incident in December 2023. USDoD supported this assertion and later reported on a hacking forum that someone else was responsible for the July 2024 leak, alleging the database had been available on underground forums and had changed hands several times since December 2023.

USDoD’s previous targets include the FBI InfraGard portal, TransUnion, Airbus, and several others. This breach may make USDoD the most infamous of cybercriminals, but they are not the main villain in this story.

In the opaque world of data brokers, it is not clear what sources their data comes from or how they associate what they collect with actual people; NPD is no different. Most of the victims of NPD likely had no idea that the company held their data in the first place. However, given the jarring lack of oversight in the industry, NPD and other companies like them don’t need the victim’s permission to host and sell their data.

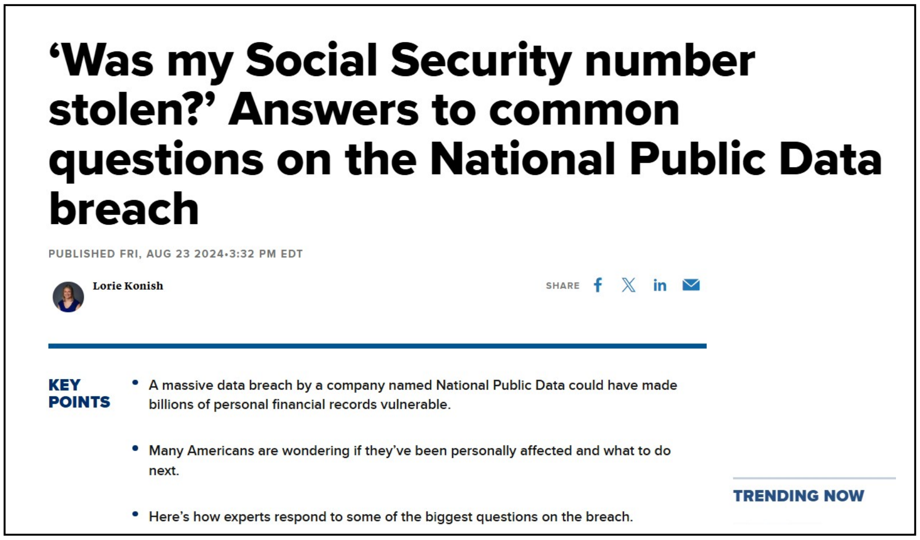


National Public Data confirms massive data breach included Social Security numbers

Social Security numbers, names, addresses, email addresses and phone numbers were in the 2.9 billion records within a data breach. Security firm Pentester.com tool tells you if your data is involved.

Mike Snider
USA TODAY

Published 5:30 p.m. ET Aug. 17, 2024 | **Updated 11:39 a.m. ET Aug. 22, 2024**



‘Was my Social Security number stolen?’ Answers to common questions on the National Public Data breach

PUBLISHED FRI, AUG 23 2024•3:32 PM EDT

Lorie Konish

KEY POINTS

- A massive data breach by a company named National Public Data could have made billions of personal financial records vulnerable.
- Many Americans are wondering if they’ve been personally affected and what to do next.
- Here’s how experts respond to some of the biggest questions on the breach.

5. Which IT Act is applicable for this Crime?

United States Laws

- **Computer Fraud and Abuse Act (CFAA)** – Prohibits unauthorized access to computer systems.
- **Federal Trade Commission Act (FTC Act)** – Holds businesses accountable for failing to protect consumer data.
- **General Data Protection Regulation (GDPR)** – If EU citizens were affected, this law mandates strict penalties for mishandling data.

India's IT Act, 2000 (Amendment 2008)

- **Section 43**: Covers hacking and unauthorized data access.
- **Section 66**: Deals with cybercrimes involving fraudulent intent.
- **Section 72A**: Punishes disclosure of personal information without consent.

6. What Ethics you have to follow in such case?

To prevent such data breaches, companies and cybersecurity professionals should adhere to the following ethical guidelines:

- **Transparency**: Companies must disclose data breaches promptly.
- **Accountability**: Organizations should take responsibility for security failures.
- **User Privacy Protection**: Sensitive information should be encrypted and stored securely.
- **Compliance with IT Laws**: Businesses must follow cybersecurity regulations to avoid legal repercussions.
- **Regular Security Audits**: Implementing frequent penetration testing and risk assessments.
- **Cybersecurity Training**: Employees should be trained to recognize phishing attempts and security threats.

7. Conclusion

The **2024 National Public Data Breach** serves as a **critical reminder** of the growing threats in the digital landscape. It highlights the **importance of data security, proactive cybersecurity measures, and strict regulatory compliance**. Organizations must strengthen their defenses against cyberattacks and prioritize user privacy to prevent similar breaches in the future. The legal consequences faced by **National Public Data** underscore the **importance of ethical responsibility in handling sensitive information**.

8. References

2024 National Public Data breach - Wikipedia

2024 National Public Data Breach | Cybersecurity Prevention

Social security number hack: National Public Data confirms data breach

Was my Social Security number stolen? National Public Data breach questions