

From: Timothy D. Shields <tshields@kelleykronenberg.com>
Sent: Saturday, August 17, 2024 7:40 PM
To: IDTheft
Subject: Breach notification- National Public Data
Attachments: NPD Breach Notification Letter 8_10.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Data breach

Hello,

National Public Data has experienced a breach that may have impacted 19027 Maryland citizens. Attached is the notification and additionally information is available on the website at <https://nationalpublicdata.com/Breach.html>.

The impacted systems have been taken offline and National Public Data is cooperating with ongoing investigations to determine the scope of the breach.

Thank you,

Timothy D. Shields, Ed.D., Esq.
Partner - Technology, Data Privacy, Social Media

10360 West State Road 84
Fort Lauderdale | FL 33324
(954) 370-9970 Ext. 1035 | Office
(954) 661-6201 | Cell
(954) 382-1988 | Fax
[Website](#) | [Email](#) | [Bio](#)



Important - Kelley Kronenberg utilizes spam and junk email filtration applications in its email information systems. These systems may prevent or delay delivery of certain email communications. If you do not receive a timely response to an email communication, please contact the intended recipient via phone in one of our office locations available [here](#).

The information transmitted, including any attachments, is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited, and all liability arising therefrom is disclaimed. If you received this in error, please contact the sender and delete the material from any computer. Thank you.

[Date]

Dear [Recipient's Name]:

We are contacting you to advise you that we have learned of a data security incident potentially involving your personal information. We want to provide you with more information below.

What Happened?

There appears to have been a data security incident that may have involved some of your personal information. The incident is believed to have involved a third-party bad actor that was trying to hack into data in late December 2023, with potential leaks of certain data in April 2024 and summer 2024. We conducted an investigation and subsequent information has come to light.

What Information Was Involved?

The information that was suspected of being breached contained name, email address, phone number, social security number, and mailing address(es).

What We Are Doing

We cooperated with law enforcement and governmental investigators and conducted a review of the potentially affected records and will try to notify you if there are further significant developments applicable to you. We have also implemented additional security measures in efforts to prevent the reoccurrence of such a breach and to protect our systems.

What You Can Do

We are notifying you so that you can take action which will assist to minimize or eliminate potential harm. We strongly advise you to take preventive measures to help prevent and detect any misuse of your information.

As a first step, we recommend that you closely monitor your financial accounts and if you see any unauthorized activity, you should promptly contact your financial institution.

As a second step, you may want to contact the three U.S. credit reporting agencies (Equifax, Experian, and TransUnion) to obtain a free credit report from each by calling 1.877.322.8228 or by logging onto www.annualcreditreport.com.

It is also recommended that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at

IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, it is recommended that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

For More Information

We understand that you may have concerns or questions.

For the latest information, please visit our website at <https://nationalpublicdata.com/breach>.

Sincerely,

National Public Data

[Date]

Dear [Recipient's Name]:

We are contacting you to advise you that we have learned of a data security incident potentially involving your personal information. We want to provide you with more information below.

What Happened?

There appears to have been a data security incident that may have involved some of your personal information. The incident is believed to have involved a third-party bad actor that was trying to hack into data in late December 2023, with potential leaks of certain data in April 2024 and summer 2024. We conducted an investigation and subsequent information has come to light.

What Information Was Involved?

The information that was suspected of being breached contained name, email address, phone number, social security number, and mailing address(es).

What We Are Doing

We cooperated with law enforcement and governmental investigators and conducted a review of the potentially affected records and will try to notify you if there are further significant developments applicable to you. We have also implemented additional security measures in efforts to prevent the reoccurrence of such a breach and to protect our systems.

What You Can Do

We are notifying you so that you can take action which will assist to minimize or eliminate potential harm. We strongly advise you to take preventive measures to help prevent and detect any misuse of your information.

As a first step, we recommend that you closely monitor your financial accounts and if you see any unauthorized activity, you should promptly contact your financial institution.

As a second step, you may want to contact the three U.S. credit reporting agencies (Equifax, Experian, and TransUnion) to obtain a free credit report from each by calling 1.877.322.8228 or by logging onto www.annualcreditreport.com.

It is also recommended that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at

IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, it is recommended that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

For More Information

We understand that you may have concerns or questions.

For the latest information, please visit our website at <https://nationalpublicdata.com/breach>.

Sincerely,

National Public Data