

**From:** Lenah Parente <lparente@penchecks.com>  
**Sent:** Thursday, October 10, 2024 11:28 AM  
**To:** Consumer  
**Cc:** Compliance Team  
**Subject:** §14–3504 Notice of a data breach - PenChecks Trust  
**Attachments:** PenChecks Trust Notice of Data Breach 10.10.2024.pdf

Dear Mr. Brown,

Pursuant to §14–3504, section h. (1), please accept this email as notification of a data breach affecting 2 (two) Maryland state residents.

PenChecks Trust is a South Dakota state chartered non-depository trust company, operating as a financial services provider in the retirement industry. Below are the incident details.

**What Information Was Involved?**

The information was an electronic file containing the 2023 IRS Form 1099-R information of 343 retirement plan participants (employees or former employees of the employer/plan sponsor). The file contained the name, address, date of birth, Social Security Number, distribution (payment) amount, and withholding tax information of the retirement plan participants.

**What Happened?**

On 9/20/2024 an authorized system user (an individual) unintentionally was able to access individuals' 1099-R information beyond that user's access permissions. The individual immediately reported their unintentional access to the appropriate persons and deleted the file. Upon learning of the incident, we began an investigation and disabled all system access so that no access would be possible until we could determine the cause and extent of the unauthorized access.

**What Are We Doing?**

After learning of the incident, we immediately deployed and followed the incident response plan, alerted the incident response team, and disabled all system access so that no unauthorized access of any kind would be possible. We then began an investigation to determine the extent of the unauthorized access and its cause. The investigation moved quickly and within 48 hours we were able to recreate the incident and identify its cause. Within 24 hours of that we coded and tested a hot-fix and then verified that the hot-fix was functioning in the production environment exactly as in the test environment and as expected. Within 12 hours of that all system access was restored and all processing resumed as normal.

The unauthorized data was accessed by one person who was authorized to have system access, but not access to the individuals' data. We have verified that that person immediately deleted the data, they made no copies of the data and we are reasonably satisfied that no copies exist outside our secure environment. Regardless, along with this Notice and out of an abundance of caution, PenChecks is offering free credit monitoring for 1 year at no charge to the affected individuals.

Attached you will find a copy of the notice being sent to the affected individuals by EOD today.

Please let us know if you have any questions, or if you require additional information.

Sincerely,

Lenah

**Lenah Parente, CAMS, CIPP/US** | Compliance & Privacy Director

PenChecks Trust

(800) 541-3938 x394 | Fax: (619) 567-8084

[PENCHECKS.com](https://penchecks.com)

We make it **simple.**



*This email is not intended to and should not be construed as providing legal, investment, tax or any other professional advice.*

**CONFIDENTIALITY & SECURITY:** *This message and all contents therein from PenChecks, Inc. and/or PenChecks Trust may be privileged, confidential or otherwise protected from disclosure under applicable law. The information is intended for the addressee only. If you have received this message in error any disclosure, copying, distribution or use of the contents of this message is prohibited. Please notify us immediately by reply email or telephone (800-541-3938), destroy the original message, all attachments and all copies. All incoming e-mail and replies are electronically filtered for spam and viruses. That filtering process may result in your email or reply being temporarily or permanently quarantined. As such, please take appropriate steps to ensure that communications of a critical nature are, in fact, received by your intended recipient(s).*

This email is not intended to and should not be construed as providing legal, investment, tax or any other professional advice.

**Confidentiality and Filtering:** This message and all contents therein from PenChecks Trust may be privileged, confidential or otherwise protected from disclosure under applicable law. The information is intended to be for the addressee only. If you have received this message in error any disclosure, copying, distribution or use of the contents of this message is prohibited. Please notify us immediately by reply email or telephone (800-541-3938), destroy the original message, all attachments and all copies. All incoming e-mail and replies are electronically filtered for spam and viruses. That filtering process may result in your email or reply being temporarily or permanently quarantined. As such, please take appropriate steps to ensure that communications of a critical nature are, in fact, received by your intended recipient(s).

**From: PenChecks, Inc./PenChecks Trust**

**Date: October 10, 2024**

**Subject: Notice of Data Breach – Limited Unintentional Disclosure**

## **PenChecks, Inc.**

PenChecks, Inc. and PenChecks Trust Company of America (“PenChecks”) takes the privacy and confidentiality of your information very seriously. We are writing to notify and update you regarding an incident involving your personal information PenChecks used to process payment of your retirement plan benefit. Based upon our investigation of this incident, we have determined that the unintentional, unauthorized disclosure of your personal information was limited and was promptly corrected and secured. The information was immediately and completely deleted by the person that unintentionally accessed it. And there is no evidence that your personal information was exposed beyond the one (1) person that unintentionally accessed it.

### **What Information Was Involved?**

The information was an electronic file containing the 2023 IRS Form 1099-R information of 343 retirement plan participants (employees or former employees of the employer/plan sponsor). The file contained the name, address, date of birth, Social Security Number, distribution (payment) amount, and withholding tax information of the retirement plan participants.

### **What Happened?**

On 9/20/2024 an authorized system user (an individual) unintentionally was able to access individuals’ 1099-R information beyond that user’s access permissions. The individual immediately reported their unintentional access to the appropriate persons and deleted the file. Upon learning of the incident, we began an investigation and disabled all system access so that no access would be possible until we could determine the cause and extent of the unauthorized access.

### **What Are We Doing?**

After learning of the incident, we immediately deployed and followed the incident response plan, alerted the incident response team, and disabled all system access so that no unauthorized access of any kind would be possible. We then began an investigation to determine the extent of the unauthorized access and its cause. The investigation moved quickly and within 48 hours we were able to recreate the incident and identify its cause. Within 24 hours of that we coded and tested a hot-fix and then verified that the hot-fix was functioning in the production environment exactly as in the test environment and as expected. Within 12 hours of that all system access was restored and all processing resumed as normal.

Your data was accessed by one person who was authorized to have system access, but not access to your data. We have verified that that person immediately deleted the data, they made no copies of the data and we are reasonably satisfied that no copies exist outside our secure environment. Regardless, along with this Notice and out of an abundance of caution, PenChecks is offering free credit monitoring for 1 year at no charge to you. More about that below.

### **What Can You Do?**

We recommend you review this guidance for additional steps you can take to help safeguard your personal information and accounts online:

- Secure your devices - Keep your security software, internet browser, and operating system up to date.

- Create and use strong passwords – At least 8 and preferably 12 or more characters using combinations of letters, numbers and special characters.
- Don't use the same or similar password for different accounts and don't share your passwords with others.
- Use multi-factor authentication (MFA) – MFA makes it harder for scammers to log in to your accounts if they do get your username and password. MFA offers extra security by requiring two or more credentials to log in to your account. Something you have like a passcode, or something you are like a scan of your fingerprint, retina or face.
- You can use various methods on your own for free, including fraud alerts, credit freeze, and
- Credit Monitoring – Out of an abundance of caution PenChecks is offering you credit monitoring for one (1) year free of charge. If you would like to take advantage of one (1) year free credit monitoring please contact us via the email address or telephone number below.
- Report suspected identity theft to your state's Attorney General (<https://www.usa.gov/state-attorney-general>) and the Federal Trade Commission (FTC).

#### **For More Information:**

- **PenChecks:**

If you have additional questions you may email us at [info@penchecks.com](mailto:info@penchecks.com) or call us at 1-800-541-3938 on weekdays from 8am to 5pm PT. You may also write to us at:

PenChecks - Attn: Compliance Dept., 8580 La Mesa Blvd., Ste 101, La Mesa, CA 91942.

For information about our privacy practices, see our [Privacy Center](#).

- **Federal Trade Commission (FTC):**

<https://www.ftc.gov/data-breach-resources>

**Bureau of Consumer Protection**

Federal Trade Commission

600 Pennsylvania Ave., NW

Washington, DC 20580

- **Credit Reporting Agencies (to place a credit freeze):**

**Equifax:**

[equifax.com/personal/credit-report-services](http://equifax.com/personal/credit-report-services)

1-800-685-1111

**Experian:**

[experian.com/help](http://experian.com/help)

1-888-397-3742

**TransUnion:**

[transunion.com/credit-help](http://transunion.com/credit-help)

1-888-909-8872

- **If you live in the state of Maryland:**

[Attorney General's Office Contact Form](#)

- **If you live in the state of North Carolina:**

<https://ncdoj.gov/public-protection/>