

-
- **Company Name** : Sanford, Pierson, Thone & Streat, PLC
 - **Date of incident**: February 13, 2024
 - **What happened**: On February 13, 2024, an organized criminal ransomware group attacked our network and may have acquired some of our data by accessing our IT system. In response, we immediately retained a cyber security firm to conduct a full investigation and forensic analysis of the incident. We also reported the incident to law enforcement and are assisting with the investigation. Importantly, we are not aware of any misuse of personal information, but the compromised information is sensitive in nature and may have been potentially exposed to others. As part of our normal business operations, we receive personal information for some of our own clients, employees and vendors, but we may also have received a potentially effected individual's personal information because they are either a customer or employee of one of our clients (such as a bank or business), their personal information was disclosed to us in a legal proceeding, or their personal information was included on a public record that was in our system. We do not sell or exchange personal information with any data brokers or outside organizations. This incident was the result of an unauthorized intrusion.
 - **Number of MD residents affected**: 5
 - **What type of information exposed**: Name, address, social security number and/or driver's license number
 - **Have you notified the effected in writing and when**: Yes, written notification letters issued/mailed on March 28, 2024

A.J. Meyer
Member



SANFORD, PIERSON, THONE & STREAT, PLC

Suite 220 | 1905 East Wayzata Boulevard | Wayzata, MN 55391

Tel: 952.404.2100 | Direct: 952.303.8910 | Fax: 952.404.2111

E-Mail: andrewm@ssmnlaw.com

Web: www.ssmnlaw.com

THE INFORMATION CONTAINED IN THIS MESSAGE IS PRIVILEGED AND CONFIDENTIAL AND IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY NAMED ABOVE. IF YOU, THE READER OF THIS MESSAGE, ARE NOT THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT YOU ARE STRICTLY PROHIBITED FROM DISSEMINATING, DISTRIBUTING OR COPYING THE

INFORMATION CONTAINED IN THIS MESSAGE. IF YOU HAVE RECEIVED THIS MESSAGE IN ERROR, PLEASE NOTIFY US BY TELEPHONE AND DELETE THE ORIGINAL MESSAGE IMMEDIATELY.

DISCLAIMER: ANY ACCOUNTING, BUSINESS, OR TAX ADVICE CONTAINED IN THIS COMMUNICATION, INCLUDING ATTACHMENTS AND ENCLOSURES, IS NOT INTENDED AS A THOROUGH, IN-DEPTH ANALYSIS OF SPECIFIC ISSUES, NOR A SUBSTITUTE FOR A FORMAL OPINION, NOR IS IT SUFFICIENT TO AVOID LEGAL OR TAX-RELATED PENALTIES. IF DESIRED, OUR FIRM WOULD BE PLEASED TO PERFORM THE REQUISITE RESEARCH AND PROVIDE YOU WITH A DETAILED WRITTEN ANALYSIS. SUCH AN ENGAGEMENT MAY BE THE SUBJECT OF A SEPARATE ENGAGEMENT LETTER THAT WOULD DEFINE THE SCOPE AND LIMITS OF THE DESIRED CONSULTATION SERVICES.



SANFORD | PIERSON
THONE | STREAM
ATTORNEYS AT LAW

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 28, 2024

L0912-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: Important Security Notification
Please read this entire letter.

Dear Sample A. Sample:

We are writing to inform you of a data security incident that may have involved some of your personal information. Although we are not aware of any actual misuse of your personal information as a result of this incident, due to the sensitive nature of the compromised personal information, we are writing to inform you of the incident, to advise you of steps to further protect your personal information, and to offer you twelve (12) months of complimentary identity monitoring services.

What Happened? On February 13, 2024, an organized criminal ransomware group attacked our network and may have acquired some of our data by accessing our IT system. In response, we immediately retained a cyber security firm to conduct a full investigation and forensic analysis of the incident. We also reported the incident to law enforcement and are assisting with the investigation. Importantly, and as stated above, we are not aware of any misuse of personal information, but the compromised information is sensitive in nature and may have been potentially exposed to others. Therefore, we encourage you to review the information provided herein, including the steps you can take to further protect your personal information. As part of our normal business operations, we receive personal information for some of our own clients, employees and vendors, but we may also have received your personal information because you are either a customer or employee of one of our clients (such as a bank or business), your personal information was disclosed to us in a legal proceeding, or your personal information was included on a public record that was in our system. We do not sell or exchange personal information with any data brokers or outside organizations. This incident was the result of an unauthorized intrusion.

What Information Was Involved? The following personal information related to you was potentially impacted: name, address and [Extra1].

What We Are Doing. Upon discovering the incident, we took the immediate steps described above, which included remediating the vulnerability that led to the intrusion before bringing our system back online. We also continue to implement additional safeguards in light of new technologies and best practices.

Protecting your information:

Although we are not aware of any impacted information that may have been misused, to help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with identity detection and resources for the resolution of identity theft. We are not

B118534

0000001



L0912-L01

permitted to enroll you in Experian's® services directly – you must complete these steps individually. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: July 1, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-918-9653** by **July 1, 2024**. Be prepared to provide engagement number **B118534** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **833-918-9653**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site. We strongly encourage you to take advantage of the services offered as a precautionary method of protecting your identity and credit. There is information on additional steps you can take to help protect your personal information below.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact the Sanford, Pierson, Thone & Strean Assistance Line at **833-918-9653**, Monday – Friday from 9 am to 9 pm Eastern Time.

Sincerely,
Courtney Strean, Chief Manager

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS TO PROTECT YOUR PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, promptly change any involved account passwords, and to review account statements, credit reports, and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

You may also contact the three major credit bureaus directly to request a free copy of your credit report. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze

TransUnion Credit Freeze

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com/credit-freeze

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 9554

Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion P.O. Box 2000

Chester, PA 19016
1-888-909-8872
www.transunion.com/fraud-alerts

Equifax P.O. Box 740256

Atlanta, GA 30348
1-800-685-1111
www.equifax.com/personal/education/identity-theft/

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will likely need to provide



some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

This notice has not been delayed by law enforcement.

For District of Columbia residents, the Attorney General can be contacted at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 202.727.3400; <https://oag.dc.gov/>.

For Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 502-696-5300.

For Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 888-743-0023.

For North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400.

For New York residents, the Attorney General can be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; <https://ag.ny.gov/>. The New York State Division of Consumer Protection can be contacted at: New York State Division of Consumer Protection, 123 William Street, New York, NY 10038-3804, or Once Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001; 800-697-1220; <https://www.dos.ny.gov/consumerprotection/>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.