

[Extra3]

1 1 63 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L05

[Extra2] [Extra5]

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



February 26, 2026

[Extra1]

Dear Sample A. Sample:

At Jeff Anderson & Associates PA (“JAA”), we place the utmost importance on the trust you have in us and the confidentiality of your information. We are writing to tell you about a data incident that happened at our firm. None of your information was made public and we have no reason to believe that it ever will. But we want to let you know what happened, what we did about it, and what we are doing going forward. We recognize that this news may be concerning, and we want to assure you that we are here to support you. Please read the information below about the steps you can take to protect your identity should you feel it is appropriate.

**What Happened?**

In September 2025, we detected suspicious activity involving certain computer systems within our firm. Unfortunately, we now understand that this same cybersecurity event has impacted thousands of reputable organizations that rely upon the same firewall protection technology. We immediately engaged leading cybersecurity specialists to investigate and determine the nature and scope of the incident. The investigation revealed that on September 18, 2025, an unauthorized party gained access to parts of our computer environment and copied certain data. Once we identified the impacted data, we undertook a comprehensive review to determine what information was involved and to whom it related. Our comprehensive review ended on December 8, 2025, and are now reaching out to you directly.

**What Information Was Involved?**

Our review determined that the following information related to you was present in the potentially impacted data: your [Extra4]. Importantly, at this time, we have no evidence that your information has been made public or misused as a result of this incident and we have no reason to believe that it ever will.

**What Are We Doing?**

Protecting the privacy and security of your information is deeply important to us at JAA. We have and will continue to invest in the latest technology and training to help secure our systems. In response to this incident, we took immediate steps to secure our systems and have implemented additional safeguards to help prevent a similar event in the future. We also notified law enforcement with the hopes that this same type of intrusion could be prevented for others. Our firm also continues to undergo regular and thorough cybersecurity vulnerability testing and assessments from third-party experts. In addition, we are also offering you complimentary credit monitoring services for 24 months through Experian, as an added precaution. Please see the enclosed instructions for how to enroll in these services.

## **What Can You Do?**

We encourage you to remain vigilant by reviewing your account statements and monitoring your credit reports for any unusual activity. You can review the enclosed *Steps You Can Take to Help Protect Your Information* to learn more about helpful tips on steps you can take to protect against possible information misuse. You may also enroll in the complimentary credit monitoring services we are offering.

## **We Are Here to Help.**

We recognize that you may have questions or concerns that are not addressed in this letter. Please do not hesitate to contact us at 866-303-2281, [dataincident@andersonadvocates.com](mailto:dataincident@andersonadvocates.com) or write to us at Jeff Anderson & Associates PA, 366 Jackson Street, Suite 100, St. Paul, MN 55101. Our team is ready to assist you and answer any questions you may have.

We are sorry that we had to deliver this news and recognize that it could cause concern. We will continue to do everything to help you in this process.

Sincerely,

Jeff Anderson & Associates PA

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 24 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](http://www.ExperianIDWorks.com/restoration).

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by June 30, 2026** (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 that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-745-1682 by June 30, 2026. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR 24-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.<sup>1</sup>
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists 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.
- **\$1 Million Identity Theft Insurance<sup>2</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

---

<sup>1</sup> Offline members will be eligible to call for additional reports quarterly after enrolling.

<sup>2</sup> 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.

## **Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/data-breach-help">https://www.transunion.com/data-breach-help</a>
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

## **Additional Information**

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

