

Jason M. Schwent
T (312) 985-5939
Email:jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

March 10, 2025

VIA ELECTRONIC MAIL

The Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

We represent Professional Law Enforcement Association Inc. (“PLEA”) with respect to a data security incident involving unauthorized access to personal information as described below. PLEA takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On or around September 26, 2024, PLEA discovered suspicious activity on its systems. PLEA immediately disconnected those systems, began an investigation, and engaged independent computer forensic experts to assist. The investigation found that there had been unauthorized access to files and folders in the PLEA environment. PLEA reviewed those files and folders impacted by the incident and determined on February 6, 2025 that personal information was present in the affected files and folders.

Potentially impacted information included names, addresses, dates of birth, Social Security numbers, driver’s license or state ID numbers, financial account numbers, payment card information, medical information, and health insurance policy numbers.

2. Number of Maryland residents affected

One hundred and eight (108) residents of Maryland were notified of the incident. Notification letters were sent to potentially affected individuals on March 10, 2025. A copy of the template notification letter is attached as Exhibit A.

3. Steps taken in response to the incident

Since the incident, PLEA changed passwords and implemented additional restrictions on accessing this system, among other measures. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through TransUnion.

4. Contact information

PLEA takes the security of the information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason M. Schwent
Member

cc: Sunaina Ramesh



Professional Law Enforcement Association, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS411



March 10, 2025

NOTICE OF DATA SECURITY Incident

Dear [REDACTED],

This letter informs you of a recent data security incident that may have impacted some of your personal information stored on Professional Law Enforcement Association Inc.'s ("PLEA") systems.

PLEA takes the privacy and security of personal information seriously. This letter contains information about steps you can take to protect your information, and resources the PLEA will make available to help you.

What Happened?

On or around September 26, 2024, PLEA discovered suspicious activity on its systems. PLEA immediately disconnected those systems, began an investigation, and engaged independent computer forensic experts to assist. The investigation found that there was unauthorized access to files and folders in the PLEA environment. PLEA reviewed those files and folders and determined on February 6, 2025 that your personal information was present in the affected files and folders. We have no evidence that any information impacted by this incident was used for any illegal purpose. PLEA, however, wanted to let you know about this under an abundance of caution.

What Information Was Involved?

From PLEA's review, it appears that your [REDACTED]

[REDACTED] may have been affected.

What We Are Doing:

PLEA wants to assure you that it is taking steps to minimize the risk of this happening in the future. Since the incident, PLEA changed passwords and implemented additional restrictions on accessing this system, among other measures. In addition, while PLEA is not aware of any misuse of personal information, PLEA has arranged for you to receive Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you

become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Again, at this time, there is no evidence that personal information has been misused. However, PLEA encourages you to take full advantage of this service offering. TransUnion representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your information. PLEA also encourages you to remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements.

For More Information:

If you have questions regarding the incident, please call [REDACTED], Monday through Friday, 8:00 am – 8:00 pm Eastern Standard Time. Protecting personal information remains PLEA's top priority.

Sincerely,

Professional Law Enforcement Association Inc.

Recommended Steps to help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. 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 should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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, Telephone: 1-888-743-0023.

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 a violator. 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 0 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.