



Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

January 10, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Pachuta & Kammerman PLLC - Security Breach Notification

Dear Mr. Brown:

We are writing on behalf of our client, Pachuta & Kammerman PLLC (“Pachuta & Kammerman”) (located at 3541 Chain Bridge Road, Suite 208, Fairfax, VA 22030) to notify you of a data security incident involving one (1) Maryland resident. By providing this notice, Pachuta & Kammerman does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature

On or around November 1, 2023, Pachuta & Kammerman identified suspicious activity on its network associated with its payroll platform. After discovering the incident, Pachuta & Kammerman engaged our firm and third-party independent cybersecurity experts to conduct a thorough investigation of the nature and scope of the incident and to assist in the remediation efforts.

Pachuta & Kammerman recently concluded its initial investigation, which revealed that an unauthorized actor likely gained access to the payroll platform between October 20, 2023 and November 1, 2023 and, as a result, potentially viewed or obtained some payroll information. After concluding an extensive forensic investigation and review on January 3, 2024, Pachuta & Kammerman discovered that certain personal information was included within the payroll data that was potentially subject to unauthorized access or acquisition as a result of the incident. On January 5, 2024, Pachuta & Kammerman PLLC identified the most recent contact information for these individuals and determined that the incident involved one (1) Maryland resident.

The personal information obtained potentially included first and last name in addition to one or more of the following data elements: name, address, date of birth, Social Security number, and direct deposit routing number and account number.

Notice and Pachuta & Kammerman's Response to the Event

On January 11, 2024, Pachuta & Kammerman will mail a written notification to the potentially affected Maryland resident, pursuant to Md. Code Ann., Com. Law § 14-3501-3508, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Pachuta & Kammerman is providing the potentially impacted individual the following:

- Free access to credit monitoring services for one year through TransUnion;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, Pachuta & Kammerman provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary). Finally, Pachuta & Kammerman is working to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

January 11, 2024

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Pachuta & Kammerman PLLC. We are writing with important information regarding a recent data security incident that we initially alerted you to a few weeks ago that may have involved some of your personal information. We want to follow up on our previous correspondence to provide you with additional information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

On or around November 1, 2023, we became aware of suspicious activity in connection with our payroll platform, Paychex, involving unauthorized requests to access the Paychex platform and change direct deposit information.

What We Are Doing

Upon learning of this issue, we immediately took steps to contain the threat, promptly removed unauthorized access, and secured our systems. We also launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to ensure the security of our systems and help determine whether any sensitive data had been compromised as a result of the incident.

At the conclusion of the investigation, we determined that an unauthorized actor likely gained access to one of our Paychex accounts between October 20, 2023 and November 1, 2023 and, as a result, potentially viewed or obtained your personal information. Based on the results of our investigation and the nature of the unauthorized activity, we believe this was solely an attempt to misdirect employee payments (which, to the best of our knowledge, was not successful), and we have no evidence that your information has been used for identity theft or financial fraud. However, we wanted to notify you of the incident out of an abundance of caution and provide you information on how to best protect your identity.

What Information Was Involved

The impacted files contained your [REDACTED]
[REDACTED]

What You Can Do

As stated above, while we have no evidence indicating that your information has been used for identity theft or fraud, we strongly recommend that you remain vigilant in monitoring and reviewing all of your financial and account statements, and report any unusual activity to the institution that issued the record, as well as law enforcement. In addition, please see “**OTHER IMPORTANT INFORMATION**” on the following pages for guidance on how to best protect your identity.

Finally, we are offering a complimentary 12-month membership for credit monitoring. For more information on identity theft prevention and credit monitoring, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. If you have any further questions regarding this incident, please contact [REDACTED] at [REDACTED] or [REDACTED]

Sincerely,

Pachuta & Kammerman PLLC
3541 Chain Bridge Road, Suite 208
Fairfax, VA 22030

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

In response to the incident, we are providing you with access to 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 through Identity Force, a TransUnion company.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] 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.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.