WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

April 12, 2024

Brian H. Myers
202.626.7695 (direct)
Brian.myers@wilsonelser.com

<u>Via Email</u>

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving Payroll Select Services, LLC

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Payroll Select Services, LLC ("PSS"), a payroll processing company based in Toledo, Ohio, with respect to a recent cybersecurity incident (hereinafter, the "Incident").

This letter will serve to inform you of the nature of the Incident, what information may have been affected, the number of Maryland residents being notified, and the steps that PSS has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially affected individuals, which includes an offer of free credit monitoring services. By providing this notice, PSS does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

1. Nature of the Incident

On September 7, 2023, PSS detected unusual activity on their network. Upon discovery of this incident, PSS immediately disconnected all access to the network and promptly engaged third-party cybersecurity professionals to assist with securing PSS' environment and conducting a forensic investigation. PSS's investigation found evidence that some PSS files were accessed by an unauthorized actor.

Based on these findings, PSS reviewed the affected systems to identify the specific individuals and the types of information that may have been affected. While PSS investigated the specific individuals who may have been affected, PSS posted a public notice of the incident on their website on October 20, 2023.

Although PSS is unaware of any fraudulent misuse of information, it is possible that individuals' names, addresses, dates of birth, financial information including banking and billing information, and social security numbers may have been accessed as a result of this unauthorized activity.

As of this writing, PSS does not have any evidence indicating that any personal information has been misused for identity theft or fraud in connection with this incident.

2. Number of Maryland residents affected.

PSS identified and notified 17,337 individuals potentially affected by this Incident. Of those, seven (7) are residents of Maryland based on the most recent address information available to PSS. PSS mailed notification letters to these individuals on March 28, 2024. A sample copy of the notification letter is included with this letter as **Exhibit A**.

3. Steps taken in response to the Incident.

PSS is committed to the security and privacy of personal information in its possession, and PSS has taken steps to further improve the security of its information technology systems and practices. Upon discovery of the Incident, PSS moved quickly to investigate and respond to the Incident, assess the security of its systems, and notify the potentially affected individuals. PSS engaged specialized cybersecurity professionals to conduct a forensic investigation. PSS reset passwords, installed additional threat hunting and endpoint detection and response technologies, reconfigured certain portions of its network, increased its employee training, and is updating its policies and procedures. PSS will continue to take steps to protect the security and privacy of personal information in its possession.

PSS also offered 12 months of complimentary credit monitoring and identity theft restoration services through TransUnion to all affected individuals to help protect their identity. Additionally, PSS provided guidance to affected individuals on how to protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

PSS remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Brian.myers@wilsonelser.com or 202-626-7695.

Regards,

Wilson Elser Moskowitz Edelman & Dicker LLP

Brian H. Myers, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.

EXHIBIT A

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

PAYROLLSELECT SERVICES LLC

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

March 28, 2024

Re: Notice of Data <<custom field 1>>

Dear <First Name> <Last Name>,

Payroll Select Services, LLC ("PSS") is writing to inform you of a recent data security incident (the "Incident") that may have resulted in unauthorized access to your sensitive personal information. We are providing you with details about the Incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

<u>What Happened</u>?

On September 7, 2023, PSS was the victim of a cybersecurity incident to its local network. Upon discovery of this Incident, PSS promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. The investigation concluded on December 28, 2023, and we finalized the list of individuals that needed to be notified on March 12, 2024. Out of full transparency, PSS is providing notice about the potential access to sensitive information by an unauthorized actor. Of note, this incident did not impact the network containing payroll software.

<u>What Information Was Involved</u>?

We are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information related to you may have been subject to unauthorized access: names, addresses, dates of birth, financial information including banking and billing information, and social security numbers.

<u>What We Are Doing</u>

Data privacy and security is among PSS's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, PSS moved quickly to investigate, respond, and confirm the security of our systems. Specifically, PSS has reset passwords, deployed additional monitoring services, reconfigured certain portions of its network and is reviewing training and updating it policies and procedures as well as employee trainings. PSS also engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident.

In light of the incident, we are also 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 <<service length>> 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 TransUnion through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/pss** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>**.

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.

We encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-833-972-2152 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

PSS sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Mark Miller
Payroll Select Services, LLC

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 at 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.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226 or 1-919-716-6000; www.ncdoj.com