

Reena R. Bajowala
Tel 312.456.1018
Fax 312.874.8636
reena.bajowala@gtlaw.com

December 30, 2024

Attorney General Anthony G. Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notification of Security Incident

Dear Attorney General Brown:

We are writing to inform you that our client, American Payroll Institute Inc. (d/b/a PayrollOrg) ("PAYO"), is notifying approximately twelve (12) residents of a data security incident that may have impacted some of their personal information. PAYO is a non-profit organization that educates clients on payroll industry standards.

On October 8, 2024, PAYO discovered unexpected activity on its systems. PAYO immediately launched an investigation, which included bringing in outside cyber forensic experts. PAYO also notified and are working with federal law enforcement. The initial investigation concluded on November 14, 2024, while the investigation of the potentially compromised files continued. With the help of the experts, PAYO determined that an unauthorized third party gained access to and encrypted PAYO's systems, and may have acquired certain files containing information about its employees and contractors during the September 18, 2024 to October 8, 2024 time frame.

After conducting a detailed review of the files, which PAYO completed on December 10, 2024, PAYO identified that certain data associated with its employees and contractors was included in those files. The affected information included name, social security number, driver's license number, and payment card number. PAYO has no indication that any personal information has been misused as a result of the incident.

PAYO takes the security of personal information very seriously and has taken steps to prevent a reoccurrence. PAYO took immediate steps to contain the incident upon discovery, including resetting passwords of compromised accounts and proactively taking servers offline. Before bringing servers online, PAYO worked with outside experts to methodically assess and sign off

Office of the Attorney General

December 30, 2024

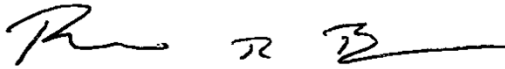
Page 2

on each server's security. PAYO is continuing to evaluate and enhance its systems, security and practices.

PAYO is mailing the attached notification to all potentially affected individuals beginning December 31, 2024.

Please contact me for any additional information.

Best Regards,

A handwritten signature in black ink, appearing to read 'Reena Bajowala', followed by a horizontal line.

Reena Bajowala
Shareholder

Schedule A
Individual Notification Letter

PayrollOrg
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P



December 31, 2024

NOTICE OF DATA BREACH

Dear



American Payroll Institute Inc. d/b/a PayrollOrg ("PAYO") takes the privacy and confidentiality of your information very seriously. We are writing to advise that PAYO recently experienced a cyber security incident which involved some of your personal information. Below is further information about the incident and our response, as well as the steps you can take to protect your information, including signing up for a credit monitoring service we are providing free of charge.

What happened?

On October 8, 2024, PAYO discovered unexpected activity on its systems. PAYO immediately launched an investigation, which included bringing in outside cyber forensic experts. With the help of the experts, we determined that an unauthorized third party gained access to and encrypted PAYO's systems, and may have acquired certain files containing information about our employees and contractors. After conducting a detailed review of the files, we identified that certain data associated with you was included in those files.

We have received no reports of identity theft or other misuse of information in relation to this incident, and have taken all steps available to protect the information from further disclosure. However, out of an abundance of caution, we are providing you with information about the resources we have brought on and the measures you can take to help protect your information.

What information was involved?

Our investigation determined that the files potentially acquired contained the following types of personal information about our current and past employees and contractors: Name, Social Security Number.

What we are doing.

Upon discovery of the incident, PAYO promptly launched our investigation with forensic experts. We also notified and are working with federal law enforcement. This notice has not been delayed by law enforcement. PAYO took immediate steps to contain the incident upon discovery, including resetting passwords of compromised accounts and proactively taking servers offline. Before bringing servers online, PAYO worked with outside experts to methodically assess and sign off on each server's security. PAYO is continuing to evaluate and enhance its systems, security and practices.

What you can do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and potential errors, and to report suspected identity theft incidents to local law enforcement or your state's attorney general. Also, we encourage you to carefully review the attached *Steps You Can Take to Protect Your Information*, and to enroll in the identify protection services that we are offering

000010102G0500

P

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 24 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. Please note PAYO is not permitted to enroll you in these services, so you will need to follow instructions below to do so.

We are also providing you with proactive fraud assistance to help with any questions that you might have or in the 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.

How do I enroll for the free services?

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: **ED2C8874966D**. 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 your information for your own protection to confirm your identity.

What if I want to speak with PAYO regarding this incident?

Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

At PAYO, we take our responsibilities to protect your information seriously. We regret the inconvenience caused by this situation.

Sincerely,

PAYO

660 North Main Avenue, Suite 100

San Antonio, TX 78205.

Phone: +1.210.224.6406

Steps You Can Take to Protect Your Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

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



Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, 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 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 have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (<https://www.transunion.com/fraud-alerts>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also 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 by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-reports-services/credit-freeze/
1-866-478-0027

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
<http://www.experian.com/freeze/center.html>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft.

District of Columbia Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Attorney General
400 6 th Street NW Washington, DC 20001 1-202-442-9828 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence RI 02903 1-401-274-4400 https://riag.ri.gov/