

Office of the Attorney General of Maryland
Attn: Security Breach Notification
200 St. Paul Place Baltimore, MD 21202



VIA U.S. Mail

July 31, 2023

Dear Sir or Madam:

We write on behalf of Paycom Payroll, LLC ("Paycom"), 7501 W Memorial Rd. Oklahoma City, OK 73142. Pursuant to MD Code Ann. Comm. Law 14-3504, we write to notify you of an incident that affects the security of information relating to twenty-two (22) Maryland residents. By providing this notice, Paycom does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Progress Software Corporation ("Progress") recently announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform, that allowed an unauthenticated attacker to gain access to MOVEit databases. It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software. Upon learning of the vulnerability, Paycom blocked the IP addresses known to be associated with the incident and made all necessary security updates to the MOVEit software.

On July 13, 2023, Paycom learned its MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023, and June 2, 2023. Paycom immediately engaged data privacy counsel and a third-party computer forensics team to investigate and determine the full nature and scope of the compromise. Paycom also notified law enforcement of the MOVEit incident and will cooperate with any investigation. There is no indication the incident impacted Paycom's HR and payroll software application. Paycom no longer uses the MOVEit file transfer software.

After completing a thorough investigation of the incident, Paycom determined that the information impacted by the MOVEit incident includes personal information for Maryland residents who are current or former employees of Paycom or their dependents. The impacted data contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information. Paycom is accordingly notifying twenty-two (22) affected Maryland individuals on July 31, 2023, via U.S. Mail. Out of an abundance of caution, Paycom is providing affected individuals with identity monitoring services for 24 months. Paycom is also automatically enrolling impacted current employees and their dependents in a company benefit that further

protects their identity at no cost to the employees. A sample notice that contains instructions on activating the complimentary services is enclosed.

Paycom is reviewing its written information security program and other policies and procedures regarding data security and will implement any necessary changes as a result of the MOVEit compromise.

For further information, please do not hesitate to contact me.

Sincerely,

Sincerely,

A handwritten signature in black ink, appearing to read 'Tim Newman'.

Timothy A. Newman
timothy.newman@haynesboone.com
Direct Dial 214-651-5029

Return Mail Processing
PO Box 999
Suwanee, GA 30024

26 1 7422 *****AUTO**5-DIGIT 73142

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



July 31, 2023

Re: Notice of Progress' MOVEit Incident

Dear Sample A. Sample:

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To protect your identity, we are also enrolling you and your dependents in identity monitoring protection services offered by LegalShield. This benefit will be available to you at no cost. Additional information on this benefit will be sent and can also be found in the Paycom app under the benefits tab.

We are also offering a complimentary 24-month membership of Experian®'s IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: November 30, 2023** (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 or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023**. Be prepared to provide engagement number **B100009** 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.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.²

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. 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 (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).

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact Paycom's HR team by using Ask Here in the Paycom App and using IDShield Enrollment. You may also call 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number B100009.

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian®'s IdentityWorksSM, which are provided as a complimentary 24-month membership. To start monitoring your personal information, please follow the steps above.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. 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.

Equifax
P.O. Box 740241
Atlanta, GA 30348
888-378-4329
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-916-8800
www.transunion.com

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.

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Additional Information: 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.

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.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, <https://www.oag.dc.gov/>, 1-202-727-3400.

Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any 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.

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/> or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

Rhode Island Residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There is 1 Rhode Island resident impacted by this event.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, the consumer reporting bureaus 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 violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.