

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Amanda Ruggieri
ARuggieri@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

June 28, 2024

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for The Time Group, Inc. ("Time Group") located at 701 Cathedral Street, Baltimore, MD 21201 and write to inform you of a data security incident. By providing this notice, Time Group does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On December 21, 2023, Time Group became aware of a network intrusion that affected a limited number of systems. Upon discovery, Time Group immediately took steps to secure the network and engaged a third-party team of forensic experts to determine the full nature and scope of the incident. After a thorough investigation, Time Group discovered that a limited amount of information related to current and former employees, kept in the normal course of business, may have been accessed by an unauthorized third party in connection with this incident. On June 18, 2024, following a thorough review, Time Group confirmed that information related to two thousand five hundred and fifty-five (2,555) Maryland residents may have been accessed by an unauthorized party in connection with this incident. The information was limited to first and last name in combination with Social Security number, driver's license number, medical information, health insurance information, and/or banking information.

On June 28, 2024, Time Group sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twenty-four (24) months. The notice letter sent to the individuals is substantially similar to the letter attached hereto as Exhibit "A."

If you have any questions, please contact me.

Very truly yours,



Amanda Ruggieri, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

The Time Group, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



June 24, 2024

RE: *Important Security Notification. Please read this entire letter.*

Dear [REDACTED]

The Time Group, Inc. ("Time Group"), common paymaster for Time Group, WPM, Lighthouse, Washington Place Equities, and Madison Capital, writes to notify you of an incident that may have impacted some of your personal information as described below.

Time Group takes the privacy and security of information in its care very seriously. Currently, there is no evidence to suggest that any information has been fraudulently misused. We believe that our prompt action in fortifying our systems and safeguarding our Associates' personal information will thwart any potential future misuse. However, in an abundance of caution, Time Group is providing you with information about this incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened:

On or around December 21, 2023, Time Group experienced a network intrusion that affected a limited number of systems. Upon discovery, Time Group immediately took steps to secure its network and engaged a third-party forensic firm to investigate the incident. Following a full and thorough investigation, Time Group determined that personal information related to current and former employees, kept in the normal course of business, may have been accessed by an unauthorized third party in connection with this incident.

What Information Was Involved:

The potentially accessed information may have included your first name or initial and last name, in combination with your [REDACTED]

What Are We Doing:

Time Group has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, Time Group immediately took steps to secure its network and undertook a thorough investigation. Additionally, Time Group continues to work to further enhance the security of its network.

As an additional safeguard for your information, Time Group has arranged for you to enroll, at no cost to you, in an online credit monitoring service for 24 months provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Due to state and federal privacy laws, Time Group cannot enroll you directly. If you wish to take advantage of this complimentary credit monitoring service, you must enroll yourself.

000010102G0500

P

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, Time Group recommends that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, notify your financial institution or company if applicable, and take any additional steps needed to protect your account. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. Please review the enclosed “Steps You Can Take to Help Protect Your Information” for additional resources.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at 1-833-538-7346 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays). You can also write us at 701 Cathedral Street, Baltimore, MD 21201.

Time Group takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured that we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Justine Fields, CFO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring 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:



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.



Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.