



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 29, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Timex Group USA, Inc. (“Timex Group”) located at 555 Christian Road, Middlebury, CT, 06762, and are writing to notify your office of an incident that may affect the security of certain personal information relating to ten (10) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Timex Group does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 5, 2023, Timex Group discovered suspicious activity in its environment. Upon learning this, Timex Group immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that Timex Group was the victim of a sophisticated cyber attack, and as a result there was unauthorized access to its environment between June 1, 2023 and June 5, 2023. The investigation also determined that an unauthorized actor was able to access or take certain information stored on the network during this period of time. Therefore, Timex Group undertook a comprehensive review of the data that was accessed and/or taken to determine if any sensitive information was affected and to whom it related. On December 14, 2023, Timex Group determined the data contained certain personal information related to its current and former employees.

The information that was affected by this incident includes

Notice to New Hampshire Residents

On or about January 29, 2024, Timex Group provided formal written notice of this incident to ten (10) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Timex Group moved quickly to investigate and respond to the incident, assess the security of Timex Group systems, and identify potentially affected individuals. Timex provided a preliminary notice of this incident to current employees on or about June 16, 2023, which included an offer of complimentary credit monitoring. Further, Timex notified federal law enforcement regarding the event. Timex Group is also working to implement additional safeguards and training to its employees. Although it has no evidence of actual fraud or misuse of personal information in connection with this incident, Timex Group is providing access to credit monitoring services for _____, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Timex Group is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Timex Group is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Timex Group is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at _____.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/crm
Enclosure

EXHIBIT A

Via First-Class Mail



January 29, 2024

NOTICE OF SECURITY INCIDENT

[Redacted]

Timex Group USA, Inc. (“Timex Group”) writes to notify you of an incident that affects the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? On June 5, 2023, Timex Group discovered suspicious activity in our environment. Upon learning this, we immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that we were the victim of a sophisticated cyber-attack, and as a result there was unauthorized access to our environment between June 1, and June 5, 2023. The investigation also determined that an unauthorized actor was able to access or take certain information stored on the network during this period of time. Therefore, Timex Group undertook a comprehensive review of the data that was accessed and/or taken to determine if any sensitive information could be affected and to whom it related. On December 14, 2023, we determined the data contained certain information related to you.

What Information Was Involved? The type of information potentially impacted by this incident includes your

What We Are Doing. Timex Group takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the incident, we immediately commenced an investigation and took steps to implement additional safeguards to help prevent a similar incident from occurring in the future. We are also reviewing our policies and procedures relating to data privacy and security.

In an abundance of caution, Timex Group is providing you with access to [Redacted] of credit monitoring and identity protection services through Cyberscout, a TransUnion company, at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services. If you already activated your credit monitoring services prior to receiving this letter, the enrollment code can only be activated one time. You do not need to re-enroll in the services once activated.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through TransUnion. We also 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 activity.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, or need assistance, please call 1-844-924-4094, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. You may also write to Timex Group at 555 Christian Road, Middlebury, CT 06762.

Sincerely,

David Payne
Senior Vice President General Counsel, HR, and Secretary
Timex Group USA, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in 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 _____ 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 specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/timexgroup> 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

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers 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 display on a consumer’s credit file, 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, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. 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 and your state Attorney General. 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 www.marylandattorneygeneral.gov.

For New Mexico residents, 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 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 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 by visiting 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 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.

For 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 incident. There are 26 Rhode Island residents impacted by this incident.