



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

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

September 19, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent TradeZero America Inc. ("TradeZero") located at 251 Little Falls Drive, Wilmington, Delaware, 19801, and write to notify your office of an incident that may affect the security of certain personal information relating to two hundred sixty-eight (268) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TradeZero does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around July 29, 2024, TradeZero learned of suspicious activity affecting the environment of its third-party vendor, Tawk.To. TradeZero launched an investigation to determine the nature and scope of the incident. Through the investigation, it determined that an unauthorized actor may have had access to certain files associated with customer communications that were contained on the Tawk.To platform. On or about August 9, 2024, TradeZero identified customer information was present within the records. Although TradeZero has no evidence of any identity theft or fraud in connection with this incident, TradeZero is notifying those individuals whose information was present in its systems at the time of the incident.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, financial brokerage and bank account information, and passport number.

Notice to Maryland Residents

On or about September 19, 2024 TradeZero provided written notice of this incident to two hundred sixty-eight (268) Maryland 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, TradeZero moved quickly to investigate and respond to the incident, assess the security of TradeZero systems, and identify potentially affected individuals. Further, TradeZero notified federal law enforcement regarding the event. TradeZero is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TradeZero is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TradeZero 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.

TradeZero is providing written notice of this incident to relevant state and federal 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 (267) 930-4888.

Very truly yours,

Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/hkl
Enclosure

EXHIBIT A



September 19, 2024

NOTICE OF SECURITY INCIDENT

Dear

TradeZero America Inc. (“TradeZero”) writes to notify you of an incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around July 29, 2024, TradeZero learned of suspicious activity affecting the environment of its third-party vendor, Tawk.To. TradeZero immediately launched an investigation and determined that an unauthorized actor may have had access to personal information contained in certain files associated with customer communications that were contained on the Tawk.To platform. Although we have no evidence of any identity theft or fraud in connection with this incident, TradeZero is notifying those individuals whose information was present within the potentially impacted platform.

What Information Was Involved? Our investigation determined the following types of your information may have been impacted by this incident: your name, Social Security number, driver’s license number, financial brokerage and/or bank account information, and passport number. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. Data privacy and security are among TradeZero’s highest priorities, and there are extensive measures in place to protect information in TradeZero’s care. Upon discovery, TradeZero promptly commenced an ongoing investigation to confirm the nature and scope of this incident. This investigation and response include confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities, as required by law.

As an important precaution, we are also offering twelve (12) months of complimentary access to credit monitoring services through Cyberscout, a TransUnion company. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

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. We encourage you to reset your TradeZero account password and implement two factor authentication with respect to your account. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you. While TradeZero will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-415-2556 between the hours of 8:00 a.m. and 8:00 p.m. ET, Monday - Friday, excluding holidays. You may also write to TradeZero c/o The Corporation Trust Company, Corporation Trust Center, 1209 Orange St., Wilmington, Delaware, 19801.

Very Sincerely,

Mike Haupt

CEO

Steps You Can Take To Help Protect Your Personal Information

Enroll in Credit Monitoring and Identity Restoration Services

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 twelve (12) 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 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.



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

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals 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 they are a victim of identity theft.

00001020280000

P

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

Equifax	Experian	TransUnion
<u>https://www.equifax.com/personal/credit-report-services/</u>	<u>https://www.experian.com/help/</u>	<u>https://www.transunion.com/credit-help</u>
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and <https://oag.dc.gov/>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately forty-four (44) Rhode Island residents that may be impacted by this event.