



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

December 13, 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 Gallagher Bassett Services, Inc. located at 2850 Golf Road, Rolling Meadows, IL 60008, who acquired Total Safety Consulting (“TSC”), and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. Notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, our client 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 about February 1, 2024, TSC became aware of suspicious activity related to a server. TSC immediately launched an investigation into the nature and scope of the incident and engaged forensic specialists. TSC determined that in 2023, an unauthorized individual accessed a TSC server and accessed or exfiltrated certain data.

With the assistance of third-party specialists, TSC undertook a comprehensive programmatic and manual review of the involved data to identify the type of information affected and to whom the information related. However, after receiving initial data mining results, TSC became aware of certain affected individuals and began mailing notice letters on August 30, 2024, and September 19, 2024. No residents of Maryland were identified at the time or included in those notifications. On November 11, 2024, TSC determined that certain information related to a resident of Maryland could have been affected by this event. While TSC has no evidence of any actual or attempted misuse of information, TSC is notifying individuals in an abundance of caution.

Mullen.law

The information subject to unauthorized access includes name, Social Security number, driver's license number, and financial account information.

Notice to Maryland Resident

On or about December 13, 2024, TSC provided written notice of this incident to one (1) Maryland resident. 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, TSC moved quickly to investigate and respond to the incident, assess the security of TSC systems, and identify potentially affected individuals. Further, TSC notified federal law enforcement regarding the event. TSC is also working to implement additional safeguards and training to its employees. TSC is providing access to credit monitoring services for 24 months through IDX, a Zerofox Company, to individuals whose personal information was affected by this incident, at no cost to these individuals.

Additionally, TSC is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. TSC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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 or fraud.

TSC is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/ekw
Enclosure

EXHIBIT A

Total Safety Consulting
P.O. Box 989728
West Sacramento, CA 95798-9728

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 13, 2024

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>> <<Name 2>>:

We write to notify you of an incident that affects some of your personal information. Total Safety Consulting (“TSC”) maintained your information related to past or current employment of you or a family member at TSC or a related company. Gallagher Bassett Services, Inc. purchased TSC. We take the security of information in our care seriously. While we are unaware of any actual or attempted misuse of your information, we want to provide you with information about the incident, our response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On or about February 1, 2024, TSC became aware of suspicious activity on a TSC server. We immediately launched an investigation into the nature and scope of the incident and engaged forensic specialists. We determined that an unauthorized individual accessed a TSC server in 2023.

With the assistance of third-party specialists, we undertook a comprehensive programmatic and manual review of potentially affected data. This extensive review process was undertaken to identify the type of information affected and to whom the information related. On November 11, 2024, we determined that certain information relating to you was affected. Since then, we have utilized both internal and external sources to match accurate addresses to affected individuals.

What Information Was Involved? While we have no evidence of any actual or attempted misuse of information, we are notifying you in an abundance of caution and to make you aware of the incident. Our review determined that your name and Social Security number were affected. The affected information related to you could also potentially include your driver’s license number and financial account information.

What We Are Doing. We take this incident and the security of personal information entrusted to us very seriously. Upon discovering this incident, we took immediate steps to investigate the incident. The affected server has been formally decommissioned. We have notified state and industry regulators as required. We have also notified law enforcement of this incident. As an added precaution, we are offering you, at no cost, access to 24 months of credit monitoring services, through IDX. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Protect Personal Information* for additional details on these services. Please note the deadline to enroll is March 13, 2025.

What You Can Do. TSC encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and monitor free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Protect Personal Information* and enroll in the credit monitoring services we are offering. In addition, we encourage you to promptly report any suspected incidents of identity theft to local law enforcement, the Federal Trade Commission, and/or your state Attorney General.

For More Information. If you have questions that are not answered by this letter, you may call our dedicated assistance line at 1-833-903-3648 available Monday through Friday, 9 am to 9 pm Eastern Time, excluding major U.S. holidays. You may also write to Total Safety and Gallagher Bassett at GlobalPrivacyOffice@ajg.com, or Legal Department, 2850 Golf Road Rolling Meadows, IL 60008.

We sincerely regret that it was necessary to contact you in such circumstances. Protecting information entrusted to TSC is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

GB/TSC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit 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 1-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.

Should consumers wish to place a credit freeze or fraud alert, 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

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 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 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.