



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: jsjohnson@mullen.law

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

May 25, 2022

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

Dear Sir or Madam:

We represent Touchstone Partners (“Touchstone”) located at 8107 Birnam Wood Dr., McLean, VA 22102, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Touchstone 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 February 11, 2022, Touchstone Partners discovered unusual activity involving one (1) employee email account. Touchstone Partners promptly took steps to secure the account, and conducted an investigation, aided by third-party forensic specialists, to determine the nature and scope of the event, including any risk to data present in the email account. The investigation confirmed that the email account was accessed by an unknown individual between January 28, and February 12, 2022.

Given that the investigation could not conclusively rule out access to data within the one affected email account, in an abundance of caution, Touchstone Partners then undertook a diligent review, again aided by third-party specialists, to identify what information was present in the affected email account and therefore potentially accessible to the unauthorized individual. The first phase of this process was completed on or around April 19, 2022. Touchstone Partners thereafter worked to reconcile the information with its internal records in furtherance of identifying the individuals to whom the data related and the appropriate contact information for the relevant individuals.

Touchstone Partners completed these efforts on April 20, 2022, and worked to provide notification to potentially impacted individuals as expeditiously as possible.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maryland Residents

On or about May 25, 2022, Touchstone began providing written notice of this incident to affected individuals, which includes two (2) Maryland residents. Written notice is being provided in substantially the same form as the letters attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Touchstone moved quickly to investigate and respond to the incident, assess the security of Touchstone systems, and identify potentially affected individuals. Touchstone is also reviewing and enhancing its existing practices related to data protection and security, as well as implementing additional security measures and safeguards to protect against this type of event in the future. Further, Touchstone is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Touchstone is also notifying other relevant state regulatory authorities, as required.

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

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4005.

Very truly yours,

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ:ams
Enclosure

Exhibit *A*



Martha (Marti) Hopler ChFC®

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

<<Date>>

Re: Notice of Data Event

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

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://response.idx.us/customending>

[https://app.idx.us/account-](https://app.idx.us/account-creation/protect)

[creation/protect](https://app.idx.us/account-creation/protect)

Enrollment Code: [XXXXXXXX]

Touchstone Partners is writing to notify you of a recent event that may affect the security of some of your information. This notice provides you with information about the event, our response, and steps you may take to better protect your information, should you feel it is appropriate to do so.

What Happened? On February 11, 2022, Touchstone Partners discovered unusual activity involving one (1) employee email account. We promptly took steps to secure the account, and conducted an investigation to determine the nature and scope of the event, including any risk to data present in the email account. The investigation confirmed that the email account was accessed by an unknown individual between January 28, and February 12, 2022. Given that the investigation could not conclusively rule out access to data within the one affected email account, in an abundance of caution, we then undertook a diligent review to identify what information was present in the affected email account and therefore potentially accessible to the unauthorized individual. The first phase of this process was completed on or around April 19, 2022. We thereafter worked to reconcile the information with our internal records in furtherance of identifying the individuals to whom the data related and the appropriate contact information for the relevant individuals. We completed these efforts on April 20, 2022, and worked to provide notification to potentially impacted individuals as expeditiously as possible. We are providing this notice to you because we understand, based on our investigation, that your information was present in the impacted email account during the period of unauthorized access.

What Information Was Involved? Our investigation determined the following information relating to you was present in the impacted email account: name and [data elements]. While we have no evidence that any of your information was used for identity theft or fraud as a result of the event, we are notifying you out of an abundance of caution and providing information and resources to help protect your personal information, should you feel it appropriate to do so.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. In response to the event, we promptly took steps to secure the account, including by changing the password, and conducting a diligent investigation to confirm the full nature and scope of the event. Further, as part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to mitigate recurrence of this type of incident. We are also reviewing and enhancing our existing data privacy practices. We are also notifying relevant regulatory authorities, as required.

As an added precaution we are offering you access to twelve (12) months of credit monitoring and identity theft protection services through IDX at no cost to you. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your accounts for any unusual activity, and to report any instances of theft or fraud to law enforcement. You can also enroll to

receive the complimentary monitoring services that we are offering to you. Please also review the attached *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call us at 301-526-8900.

We take this event very seriously and sincerely regret any inconvenience or concern it may cause you.

Sincerely,

Martha Hopler, ChFC, BFA

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services



Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://response.idx.us/customending> / <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 **1-800-939-4170** 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 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 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven 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 will need to provide 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
888-298-0045	1-888-397-3742	833-395-6938
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.oag.state.md.us. Touchstone Partners is located at 8107 Birnam Wood Drive McLean, Virginia 22102.



Martha (Marti) Hopler ChFC®

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

May 25, 2022

Re: Notice of Data Event

Dear Next of Kin of <<Name 1>> <<Name 2>>:

Touchstone Partners is writing to notify you of a recent event that may affect the security of some of your loved one's information. This notice provides you with information about the event, our response, and steps you may take to better protect your loved one's information, should you feel it is appropriate to do so.

What Happened? On February 11, 2022, Touchstone Partners discovered unusual activity involving one (1) employee email account. We promptly took steps to secure the account conducted an investigation to determine the nature and scope of the event, including any risk to data present in the email account. The investigation confirmed that the email account was accessed by an unknown individual between January 28, and February 12, 2022. Given that the investigation could not conclusively rule out access to data within the one affected email account, in an abundance of caution, we then undertook a diligent review to identify what information was present in the affected email account and therefore potentially accessible to the unauthorized individual. The first phase of this process was completed on or around April 19, 2022. We thereafter worked to reconcile the information with our internal records in furtherance of identifying the individuals to whom the data related and the appropriate contact information for the relevant individuals. We completed these efforts on April 20, 2022, and worked to provide notification to potentially impacted individuals as expeditiously as possible. We are providing this notice to you because we understand, based on our investigation, that your loved one's information was present in the impacted email account during the period of unauthorized access.

What Information Was Involved? Our investigation determined the following information relating to your loved one was present in the impacted email account: name and [data elements]. Please note, we have no evidence that any of your loved one's information was used for identity theft or fraud as a result of the event.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. In response to the event, we promptly took steps to secure the account, including by changing the password, and conducting a diligent investigation to confirm the full nature and scope of the event. Further, as part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to mitigate recurrence of this type of incident. We are also reviewing and enhancing our existing data privacy practices. We are also notifying relevant regulatory authorities, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your loved one's accounts for any unusual activity, and to report any instances of theft or fraud to law enforcement. Please also review the attached *Steps You Can Take to Help Protect Your Loved One's Personal Information*.

For More Information. We understand that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call us at 301-526-8900.

We take this event very seriously and sincerely regret any inconvenience or concern it may cause you.

Sincerely,
Martha Hopler ChFC, BFA

Registered Representative, Securities offered through Cambridge Investment Research Inc. a Broker Dealer, Member FINRA/SIPC and Investment Advisor Representative, Cambridge Investment Research Advisors, Inc. a Registered Investment Advisor.
Touchstone Partners and Cambridge are not affiliated.

8107 Birnam Wood Drive · McLean · Virginia · 22102 · Office 301.526.8900

STEPS YOU CAN TAKE TO HELP PROTECT YOUR LOVED ONE'S PERSONAL INFORMATION

Monitor Your Loved One's Accounts

We recommend obtaining a copy of your loved one's credit report to review whether there are any active credit accounts that need to be closed or any pending collection notices that need to be addressed. If you have not already done so, you may also request, in writing, that your loved one's credit report is flagged with the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

A spouse or executor of the estate may request a copy of your loved one's credit report or flag your loved one's credit report with the above alert. This must be requested in writing and should include the below information:

Information Related to your loved one:

- Legal name
- Social Security number
- Date of birth
- Date of death
- Last known address
- A copy of the death certificate or letters testamentary. A letters testamentary is a document issued by a court or public official authorizing the executor of a will to take control of a deceased person's estate.

Information related to the individual requesting the information or placing the alert:

- Full name
- Address for sending final confirmation
- In the case of an executor, include the court order or other document indicating the executor of the estate

In most cases, a flag will prevent the opening of new credit accounts in your loved one's name. Mailing and contact information for the three major credit bureaus is as follows:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338). 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.oag.state.md.us. Touchstone Partners is located at 8107 Birnam Wood Drive McLean, Virginia 22102.