Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

December 28, 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 Elevate Services, Inc. ("Elevate") located at 2375 E. Camelback Road, Suite 690, Phoenix, Arizona 85016, and write to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. Elevate is providing this notification on behalf of Progressive Casualty Insurance Company and its affiliated underwriting companies (together, "Progressive"). Among other services and technology offerings, Elevate provides legal support services to law firms and insurance companies handling personal injury claims. One of Elevate's insurance company customers is Progressive, and Elevate had certain Progressive data stored on systems impacted by the event. The investigation into this matter is ongoing, and this notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, Elevate and Progressive waive no 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 March 14, 2022, Elevate became aware that certain computer systems in its environment were inaccessible as a result of malicious file encryption. Elevate immediately took steps to secure its systems and launched an investigation to determine the full nature and scope of the event. Elevate also promptly notified federal law enforcement. Through Elevate's investigation, it determined that an unknown actor gained access to a limited number of its systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, Elevate performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to which customers the information related. Elevate then further reviewed its records to confirm the identities of individuals potentially affected by the event and the Elevate customers with whom they were associated. Elevate recently completed its review, which determined that information related to certain individuals associated with Progressive data was potentially impacted. As such, Elevate mailed notice to Progressive on or about November 9, 2022, offering to notify those individuals. Progressive engaged with Elevate to understand the nature of the event, timely provided Elevate with information Elevate requested by December 10 so that Elevate could notify Progressive-associated individuals, and asked Elevate to provide notice to certain state regulatory authorities on its behalf, including your office.

The information that could have been subject to unauthorized access related to Progressive-associated individuals includes: name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver's license number, and employment information and/or compensation information.

Notice to the Maryland Resident

On December 28, 2022, Elevate provided written notice of this event to approximately one (1) Maryland resident affiliated with Progressive on its behalf. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Elevate moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals and those customers with whom they were affiliated. Further, Elevate reported the event federal law enforcement. Elevate implemented additional technical and administrative safeguards and training to its employees. Elevate is providing access to credit monitoring and identity restoration services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

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

Elevate is also providing written notice of this event on behalf of Progressive to appropriate state regulators, including your office.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jrm
Enclosure

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

Elevate Services, Inc. ("Elevate") is writing to inform you of a recent data security event that may involve some of your information. Elevate provides legal and other technology services to <<b2b_text_2Data Owner>>. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On March 14, 2022, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. We immediately took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. We also promptly notified federal law enforcement. Through our investigation, we determined that an unknown actor gained access to a limited number of our systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, we performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to whom the information related. Upon completion of the review, we then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and the Elevate customers with whom they were associated. The review recently completed.

What Information Was Involved? Although the investigation could not determine the specific impacted files, the following types of information relating to you were present on our systems during the event: your name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver's license number, and employment information and/or compensation information.

What We Are Doing. We take this event, and the security of information, very seriously. Upon becoming aware of the event, we immediately took steps to secure our systems. We also conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative processes as part of our ongoing commitment to data security. As an additional precaution, we are offering complimentary credit monitoring and identity restoration services for twelve (12) months through Kroll.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed Steps You Can Take to Protect Personal Information. There you will find more information on the credit monitoring and identity restoration services we are making available to you. While we will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (XXX) XXX-XXXX, Monday through Friday, 9:00am to 6:30pm Eastern Standard Time (except U.S. holidays). You may also write to Elevate at 2375 E. Camelback Rd., Suite 690, Phoenix, AZ 85016.

Sincerely,

[Signature]

Steve Harmon
Chief Operating Officer & General Counsel
Elevate Services, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate Identity and Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **<<b2b_text_6(ActivationDeadline)>>** to activate your identity monitoring services.*

Membership Number: **<<MembershipNumber (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 event. There are [#] Rhode Island residents impacted by this event.

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

April 18, 2023

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: Supplemental Notice of Data Event

Dear Sir or Madam:

Elevate Services, Inc. ("Elevate") writes to supplement its December 28, 2022 notice regarding an event that may affect the security of certain personal information of one (1) Maryland resident. As set forth fully in the December 28, 2022 notification, Elevate's prior notice was on behalf of one of Elevate's impacted insurance company customers. Elevate is supplementing its prior notification with this notice on behalf of Government Employees Insurance Company ("Geico"). Geico is one of Elevate's insurance company customers, and Elevate had certain Geico data stored on systems impacted by the event. There is approximately one (1) potentially affected Maryland resident affiliated with Geico.

The investigation into this matter is ongoing, and this notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, Elevate does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdictions.

Nature of the Data Event

On March 14, 2022, Elevate became aware that certain computer systems in its environment were inaccessible as a result of malicious file encryption. Elevate immediately took steps to secure its systems and launched an investigation to determine the full nature and scope of the event. Elevate also promptly notified federal law enforcement. Through Elevate's investigation, it determined that an unknown actor gained access to a limited number of its systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, Elevate performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to which customers the information related. Elevate then further reviewed its records to confirm the identities of individuals potentially affected by the event and the Elevate customers with whom they were associated. Elevate recently completed its review, which determined that Geico data was potentially impacted. As such, Elevate provided notification of the event to Geico. Elevate offered to provide notifications to potentially affected individuals for its impacted clients. Geico accepted this offer and requested Elevate also provide notification to certain state supervisory bodies on its behalf, including your office.

The information that could have been subject to unauthorized access related to Geico-affiliated individuals includes: name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver's license number, and employment information and/or compensation information.

Notice to Maryland Resident

On April 19, 2023, Elevate will be providing written notice of this event to approximately one (1) Maryland resident affiliated with Geico on its behalf. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Elevate moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals and those customers with whom they were affiliated. Further, Elevate notified federal law enforcement regarding the event. Elevate implemented additional technical and administrative safeguards and training to its employees. Elevate is providing access to credit monitoring and identity restoration services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, Elevate is providing impacted individuals with guidance on how to better protect against potential identity theft and fraud, although Elevate has not received any indication that the breached data has been used fraudulently. Elevate 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jrm
Enclosure

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<b2b_text_3(C/O Name)>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

Elevate Services, Inc. ("Elevate") is writing to inform you of a recent data security event that may involve some of your information. Elevate provides legal and other technology services to <<b2b_text_2Data Owner>>. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On March 14, 2022, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. We immediately took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. We also promptly notified federal law enforcement. Through our investigation, we determined that an unknown actor gained access to a limited number of our systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, we performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to whom the information related. Upon completion of the review, we then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and the Elevate customers with whom they were associated. The review recently completed.

What Information Was Involved? Although the investigation could not determine the specific impacted files, the following types of information may have been present on our systems during the event: your name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver's license number, and employment information and/or compensation information.

What We Are Doing. We take this event, and the security of information, very seriously. Upon becoming aware of the event, we immediately took steps to secure our systems. We also conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative processes as part of our ongoing commitment to data security. As an additional precaution, we are offering complimentary credit monitoring and identity restoration services for twelve (12) months through Kroll.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed Steps You Can Take to Protect Personal Information. There you will find more information on the credit monitoring and identity restoration services we are making available to you. While we will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (855) 624-3241, Monday through Friday, 9:00 am to 6:30 pm Eastern Standard Time (except U.S. holidays). You may also write to Elevate at 2375 E. Camelback Rd., Suite 690, Phoenix, AZ 85016.

Sincerely,

Steve Harmon
Chief Operating Officer & General Counsel
Elevate Services, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate Identity and Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6(ActivationDeadline)>>*** *to activate your identity monitoring services.*

Membership Number: **<<MembershipNumber (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 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
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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 event. There are [#] Rhode Island residents impacted by this event.

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

June 7, 2023

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: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Elevate Services, Inc. ("Elevate") located at 2375 E. Camelback Road, Suite 690, Phoenix, Arizona 85016, and write to supplement our prior notifications to your office on December 28, 2022 and April 18, 2023. Elevate's prior notifications were issued on behalf of its business customers.

Elevate recently completed its investigation and determined the event may have affected the security of personal information relating to an additional six (6) Maryland residents directly related to Elevate. By providing this supplemental notice, Elevate 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

In addition to the substantial work undertaken by Elevate to review its records, notify its business customers, and subsequently issue notice to potentially affected individuals affiliated with those customers, as described in the prior notification, Elevate was contemporaneously conducting a comprehensive and time-intensive review of potentially impacted records that contained Elevate internal data, not related to Elevate's business customers. Elevate recently completed this review on or around May 11, 2023, and determined that residents of Maryland were potentially affected by the event.

The information that could have been subject to unauthorized access for Maryland residents includes name, Social Security number, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, driver's license number, and employment information and/or compensation information.

Notice to Maryland Residents

On or about June 7, 2023, Elevate provided written notice of this event to potentially affected individuals directly affiliated with Elevate, including an additional six (6) Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Elevate moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals and business customers. Further, Elevate promptly reported the event to federal law enforcement. Elevate also implemented additional technical safeguards and training to its employees. Elevate is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

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

Elevate is also providing written notice of this event to appropriate state regulators and to the three major consumer 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) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jrm
Enclosure

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<b2b_text_3(C/O Name)>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

Elevate Services, Inc. ("Elevate") is writing to inform you of a data security event that may involve some of your information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On March 14, 2022, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. We immediately took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. We also promptly notified federal law enforcement. Through our investigation, we determined that an unknown actor gained access to a limited number of our systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, we performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to whom the information related. Upon completion of the review, we then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event. This time-intensive review concluded in May 2023.

What Information Was Involved? Although the investigation could not determine the specific impacted files, the following types of information relating to you were present on one of the impacted systems: <<b2b_text_1(name, data elements)>>.

What We Are Doing. We take this event, and the security of information, very seriously. Upon becoming aware of the event, we immediately took steps to secure our systems. We also conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative processes as part of our ongoing commitment to data security. As an additional precaution, we are offering complimentary credit monitoring and identity restoration services for twelve (12) months through Kroll.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed Steps You Can Take to Protect Personal Information. There you will find more information on the credit monitoring and identity restoration services we are making available to you. While we will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (855) 624-3241, Monday through Friday, 9:00 am to 6:30 pm Eastern Standard Time (except U.S. holidays). You may also write to Elevate at 2375 E. Camelback Rd., Suite 690, Phoenix, AZ 85016.

Sincerely,

Steve Harmon
Chief Operating Officer & General Counsel
Elevate Services, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6(ActivationDeadline)>>*** *to activate your identity monitoring services.*

Membership Number: **<<MembershipNumber (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 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 credit 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
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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 event. There are 2 Rhode Island residents impacted by this event.

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

August 4, 2023

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: Supplemental Notice of Data Event

To Whom It May Concern:

Elevate Services, Inc. ("Elevate") writes to supplement its December 28, 2022, April 18, 2023, and June 7, 2023 notices regarding an event that may affect the security of certain personal information of Maryland residents. Elevate is supplementing its prior notifications with this notice on behalf of Liberty Mutual Insurance Company ("Liberty Mutual"). Liberty Mutual is one of Elevate's insurance company customers, and Elevate had certain Liberty Mutual data stored on systems impacted by the event. There are approximately ten (10) potentially affected Maryland residents affiliated with Liberty Mutual.

This notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, Elevate and Liberty Mutual waive no 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

As previously reported, on March 14, 2022, Elevate became aware that certain computer systems in its environment were inaccessible as a result of malicious file encryption. Elevate immediately took steps to secure its systems and launched an investigation to determine the full nature and scope of the event. Elevate also promptly notified federal law enforcement. Through Elevate's investigation, it determined that an unknown actor gained access to a limited number of its systems between March 5, 2022, and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, Elevate performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to which customers the information related. Elevate then further reviewed its records to confirm the identities of individuals potentially affected by the event and the Elevate customers with whom they were associated. Upon completion of that review, Elevate determined that information related to certain individuals associated with Liberty Mutual was potentially impacted. As such, Elevate mailed notice to Liberty Mutual on or about November 9, 2022, offering to notify those individuals. Liberty Mutual engaged with Elevate to understand the nature of the event, and timely provided Elevate with information Elevate requested so that Elevate could notify Liberty Mutual-associated individuals. Liberty Mutual also asked Elevate to provide notice to certain state regulatory authorities on its behalf, including your office.

The information that could have been subject to unauthorized access related to Liberty Mutual-associated individuals includes: name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver's license number, and employment information and/or compensation information.

Notice to Maryland Residents

On or about August 4, 2023, Elevate provided written notice of this event to ten (10) Maryland residents affiliated with Liberty Mutual on its behalf. 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 becoming aware of the event, Elevate moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals and those customers with whom they were affiliated. Further, Elevate reported the event to federal law enforcement. Elevate implemented additional technical and administrative safeguards and training to its employees. Elevate is providing access to credit monitoring and identity restoration services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

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

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/jrm
Enclosure

EXHIBIT A

elevate

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<b2b_text_3(C/O Name)>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

Elevate Services, Inc. (“Elevate”) is writing to inform you of a recent data security event that may involve some of your information. Elevate provides legal and other technology services to <<b2b_text_2Data Owner>>. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On March 14, 2022, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. We immediately took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. We also promptly notified federal law enforcement. Through our investigation, we determined that an unknown actor gained access to a limited number of our systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, we performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to whom the information related. Upon completion of the review, we then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and the Elevate customers with whom they were associated. The review recently completed.

What Information Was Involved? Although the investigation could not determine the specific impacted files, the following types of information relating to you were present on our systems during the event: your name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver’s license number, and employment information and/or compensation information.

What We Are Doing. We take this event, and the security of information, very seriously. Upon becoming aware of the event, we immediately took steps to secure our systems. We also conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative processes as part of our ongoing commitment to data security. As an additional precaution, we are offering complimentary credit monitoring and identity restoration services for twelve (12) months through Kroll.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed Steps You Can Take to Protect Personal Information. There you will find more information on the credit monitoring and identity restoration services we are making available to you. While we will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (855) 624-3241, Monday through Friday, 9:00 am to 6:30 pm Eastern Standard Time (except U.S. holidays). You may also write to Elevate at 2375 E. Camelback Rd., Suite 690, Phoenix, AZ 85016.

Sincerely,

Steve Harmon
Chief Operating Officer & General Counsel
Elevate Services, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate Identity and Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6(ActivationDeadline)>>*** *to activate your identity monitoring services.*

Membership Number: **<<MembershipNumber (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 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
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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 event. There are [#] Rhode Island residents impacted by this event.