December ___, 2021

TO: GA West & Co., Inc. current and former employees

FROM: GA West & Co., Inc.

NOTICE OF DATA SECURITY INCIDENT

On October 11, 2021, GA West & Co, Inc. ("GA West" or the "Company") had reason to believe that it experienced a data incident that may have resulted in unauthorized access to various electronic files maintained by the Company. This notice is provided to alert you and provide you additional information as set out herein.

WHAT HAPPENED?

On October 11, 2021, GA West & Co, Inc. ("GA West" or the "Company") had reason to believe that it experienced a data incident that may have resulted in unauthorized access to various electronic files maintained by the Company. This notice is provided to alert you and provide you additional information as set out herein.

The Company immediately began an investigation. It retained third-party cybersecurity forensic experts and legal counsel. The investigation did not locate a ransomware note. Additionally, the investigation did not identify evidence that information, including personal information, was exfiltrated from GA West's electronic systems. While there was some evidence of encryption or corruption of various Company files, not all electronic files were affected. We are sending this notification in an abundance of caution to let you know that your personal information may or may not have been encrypted and/or corrupted. Moreover, while there is no evidence that your personal information was exfiltrated, we cannot guarantee that no personal information of any individual was exfiltrated. Additionally, and also in an abundance of caution, we are offering you the opportunity to register for one (1) year of free credit monitoring, as described further below. We are also offering a toll-free number to answer questions you may have about this incident.

WHAT INFORMATION WAS INVOLVED?

With regard to the personal information that may have be contained in the files that may have been compromised, this information includes name, postal address, telephone number, email address, driver's license number, social security number, and application for financial or healthcare benefits. We are unable to confirm the number or identity of current or former employees who may have had their personal information compromised.

WHAT WE ARE DOING

GA West values your privacy and regrets that this incident occurred. The federal Cybersecurity and Infrastructure Security Agency (CISA) is aware of this incident, and GA West has cooperated with CISA concerning this matter. To address this incident, we have implemented a number of additional security precautions, including:

- Activated the Company's internal data security response team.
- Executed additional security measures to help mitigate the risk of continued unauthorized access.
- Engaged experienced, outside forensics cybersecurity experts.
- Notification of federal agencies (CISA).

The Company has implemented the following summary of additional remediation actions thus far:

- Deployed new server infrastructure
- Deployed Antivirus protection
- Deployed Security Patch Management
- Restoration of data
- Implemented Security Best Practices, including:
  - Minimum password length/complexity
  - Password change policy/history
  - Required all users to change passwords
  - Restricted administrative access to IT Team
- Implemented new password policy
- Implemented Web Content Filtering providing additional protections
- Implemented VPN Firewall for Secure Remote Desktop Protocol (RDP) access
- Implemented Multi-Factor Access on subject services
- Segmented internal networks to reduce horizontal threat vectors
- Implemented Endpoint Detection & Response
- Enlisted Security Operations Center for monitoring of all threat vectors
- Update Firmware and reduced network protocols on network printers
- Disabled Network Basic Input/Output System (NetBIOS) over Transmission Control Protocol (TCP).

WHAT YOU CAN DO

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at <<TOLL-FREE NUMBER>> (toll free), available from 8:00 AM to 8:00 PM Central Time, except holidays.

We take the privacy and security of the personal information in our care seriously. Please let us know if you have any questions.

OFFER OF COMPLIMENTARY CREDIT MONITORING SERVICE

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to have the option to enroll, at no cost to you, in an online credit monitoring service (1-Bureau Credit Watch Gold) for one (1) year provided by Equifax, one of the three nationwide credit reporting companies.

To enroll in this service, go to the Equifax website at ***www.equifax.com/activate*** and in the space referenced as "Enter Activation Code", enter the following Activation Code **<<Insert Activation Code>>** and follow the steps to receive your credit monitoring service. Please see more information regarding the enrollment process at the end of this letter.

You can sign up for the credit monitoring service anytime between now and **<<Insert Date>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one (1) year of unlimited access to your Equifax credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

ADDITIONAL STEPS YOU CAN TAKE

As a precautionary measure, we recommend you remain vigilant by reviewing your financial account statements and monitoring free credit reports closely. If you detect any suspicious activity, you should promptly notify the relevant financial institution or credit bureau reporting the activity. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For more information, visit IdentityTheft.gov, call 877-ID-THEFT (877-438-4338), or mail the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580, using OMB CONTROL#: 3084-0169. A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Obtain and Monitor Your Credit Report

You can obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months. You may also access these reports by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided here:

Equifax	Experian	TransUnion
866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That is because most creditors need to see your credit report before they approve a new account. If they cannot see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

The mailing address for GA West is: 1200 Radcliff Road Creola, Alabama, 36525.

Additional information for residents of the following states:

Connecticut: You may contact and obtain any relevant information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave., Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain any relevant information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us.

New York: You may contact and obtain any relevant information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-6971220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain any relevant information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.