



Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David B. Sherman
direct dial: 215.564.8380
dsheer@bakerlaw.com

August 9, 2023

SENT VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Attorney General Brown:

We are writing on behalf of our client, M. Arthur Gensler, Jr. & Associates, Inc. (“Gensler”), to notify you of a security incident involving 149 Maryland residents.

The incident involved Progress MOVEit, a software vendor used by several global organizations, including Gensler, as a secure file transfer protocol (also referred to as “SFTP”). Upon receiving notice of the incident from MOVEit on May 31, 2023, Gensler immediately disabled web access to the SFTP environment, patched the exploit, and ensured its systems were secure. Outside cybersecurity firms were engaged to conduct an investigation, which determined that the incident involved an unauthorized party initially accessing the platform on May 15, 2023, and then subsequently copying certain Gensler files from the platform between May 27, 2023 and May 31, 2023. The investigation also confirmed that the incident did not impact Gensler’s internal systems. Gensler conducted a thorough review of the files involved and determined that a file contained the names and Social Security numbers of certain Gensler employees. On June 23, 2023, Gensler confirmed that 149 of those employees reside in Maryland.

On June 8, 2023, Gensler provided a preliminary notice to the involved employees via email. On August 9, 2023, Gensler mailed notification letters to the involved Maryland residents pursuant to Md. Code Ann., Com. Law § 14-3504. The letter was sent via United States Postal Service First-Class mail. A sample copy of the written notification letter is enclosed. Gensler is offering the Maryland residents a complimentary, two-year membership to credit monitoring and identity theft protection services through Experian. Gensler also notified law enforcement and

August 9, 2023

Page 2

established a dedicated call center for notification recipients to call to obtain more information regarding the incident.

To help prevent a similar incident from occurring, Gensler is implanting additional protocols to further enhance its existing security policies pertaining to the use of SFTP's.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in dark ink, appearing to read "D. B. Sherman", with a stylized flourish at the end.

David B. Sherman
Partner

Enclosure



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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

As a firm, we deeply value the relationship of trust we have with our people and our clients. We have a strong sense of responsibility for the confidential information that is shared with us and take extensive measures to protect that information. Nevertheless, as outlined in our June 8, 2023 email to you, a recent global data incident impacting a software vendor used by many prominent organizations around the world has also impacted Gensler.

The purpose of this letter is to provide a hardcopy notice describing the incident and reiterate the actions the firm has taken to date and the steps you can take to protect your personal data.

Incident Overview

The incident involved Progress MOVEit, a software vendor used by global organizations, including Gensler, as a secure file transfer protocol (also referred to as “Secure FTP”). The incident involved an unauthorized party intermittently accessing and copying certain Gensler files on the platform between May 27, 2023 and May 31, 2023.

We performed a thorough review of the involved files, and we determined that one of these files included your name, Social Security number, and date of birth. We then conducted additional research, which was completed on June 23, 2023, to gather the information needed to send this letter to you.

Actions to Protect Your Data

Upon learning of the incident, Gensler IT acted swiftly to disable web access to the FTP environment, patch the exploit, and secure our Gensler systems. We immediately began an investigation and forensic analysis and determined that personal information of our Gensler colleagues in the United States was included in the incident. We also confirmed that the incident did not impact our internal Gensler systems.

As a precaution, we arranged for you to receive a complimentary, two-year membership of identity theft protection and credit monitoring services through Experian. These services are completely free to you and enrolling in these services will not hurt your credit score. For more information on identity theft prevention, additional steps you can take in response, and instructions on how to activate your complimentary, two-year membership, please see the following pages provided with this letter.

Additional Information

Our Regional HR Directors and Regional Legal Counsel are available to provide you support and answer any questions about the incident. You may also contact our dedicated helpline at (866) 547-2294 from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding certain major U.S. holidays.

We remind you that following incidents like this, it is important to be especially vigilant with emails, calls, texts, or mail scams that ask for personal information. Suspicious messages should be forwarded to badmail@gensler.com.

Please be reassured that there is a global response team working diligently and tirelessly to take all steps possible to mitigate any potential further impact from this incident.

Sincerely,

A handwritten signature in black ink, appearing to read 'LGray', written in a cursive style.

Larissa Gray
Global Compliance Director | Gensler

ACTIVATION INSTRUCTIONS

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** <<b2b_text_6(enrollment deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **WWW.EXPERIANIDWORKS.COM/3BCREDIT**
- Provide your **activation code:** <<activation code s_n>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 288-8057 by <<b2b_text_6(enrollment deadline)>>. Be prepared to provide engagement number <<b2b_text_1(engagement number)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (877) 288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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.identitytheft.gov.

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's because most creditors need to see your credit report before they approve a new account. If they can't 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 160, Woodlyn, PA 19094, 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.

Gensler's mailing address is 500 S. Figueroa St., Los Angeles, CA 90071 and its phone number is 213-327-3600.

Additional information for residents of the following states:

Connecticut: You may contact and obtain 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.

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

Maryland: You may contact and obtain 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 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 / 1-800-697-1220, <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 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.

Rhode Island: This incident involves [#] individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

A 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 NW, 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.