



Pillsbury Winthrop Shaw Pittman LLP
725 South Figueroa Street, 36th Floor | Los Angeles, CA 90017-5524 | tel 213.488.7100 | fax 213.629.1033

Catherine D. Meyer
tel: 213-488-7362

September 19, 2024

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

By email: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Sir/Madam:

This letter is being sent in accordance with state law to inform your office that the name, Social Security Number, driver's license number and/or financial account number without access security codes of approximately 1213 Maryland residents may have been subject to unauthorized access. Not all categories of information was exposed about all individuals. Twelve months of credit monitoring has been provided to all impacted individuals through Experian IdentityWorks.

We represent The Gill Corporation, 4056 Easy Street, El Monte, CA 91731, in connection with a ransomware incident which occurred on June 23, 2024 when a threat actor exploited a vendor's application to access and encrypt some of the company's servers. While the company was able to stop the intrusion midstream, which reduced the damage that could have been done, the company was not able to discover if personal information was accessed or exposed until August 5, 2024 because the servers had been encrypted by the threat actors and a thorough forensic review was required to discover the scope of the access.

The company diligently investigated the incident including forensic review and discovery of the identities of potentially impacted individuals using skilled experts to assist on the technical side. It reported to and is fully cooperating with law enforcement and appropriate government agencies (Secret Service and FBI).

The company has notified the impacted individuals between September 13-16, 2024. We have enclosed a copy of the notice letter. The three Consumer Reporting Agencies have been notified of this incident pursuant to requirements of other states'

September 19, 2024

Page 2

laws. Notification has been delayed because the threat actor encrypted the servers and files on those servers which prevented the company from discovering whether personal information was accessed or exposed until on or after August 5, 2024, after which the company diligently worked to identify the impacted individuals, the types of data exposed, and their contact information.

Prior to the attack the network and systems were continuously monitored and regularly assessed and patched with assistance of two cyber security companies. The company is in the process of validating and hardening the security of those systems, including enhanced security to credentials, increased amount and frequency of vulnerability scans, and enhanced employee training.

Should you have any additional questions, you may contact me directly at (213) 488-7362.

Very truly yours,

A handwritten signature in cursive script, appearing to read "Catherine D. Meyer".

Catherine D. Meyer
Senior Counsel



THE GILL CORPORATION

HIGH PERFORMANCE COMPOSITE PRODUCTS SINCE 1945

September __, 2024

[Name]

[Address 1]

[Address 2]

Re: Notice of Data Breach

Dear [Name]

On behalf of The Gill Corporation ("TGC") I am writing to you about a cyber-attack on TGC that occurred in late June 2024 ("Cyber-Attack"). During the Cyber-Attack an unauthorized third party compromised TGC's systems by encrypting many TGC files and backup systems. Since the Cyber-Attack, TGC has been investigating whether, among other things, the Cyber-Attack may have resulted in the unauthorized access to and the acquisition of the personal information of former TGC employees. Although TGC's investigation is ongoing, we have reason to believe that some personal information we obtained from you in the course of your employment with TGC was accessed and taken during the Cyber-Attack. This unauthorized access likely occurred on or around June 23, 2024. We are notifying you so that you may take steps to protect yourself. We take security very seriously and deeply regret that this incident occurred.

What Information was Involved?

We began investigating the incident as soon as we learned of it. Although our investigation is ongoing, we have determined that the personal information pertaining to you that may have been involved in this incident may have included your name and Social Security Number and a limited number of driver's license numbers and/or bank account numbers. Your form W-2 for past years was likely to have been exposed.

What We are Doing.

We have identified the vulnerability that was exploited by the third party and we have removed it from TGC's systems. We have already deployed additional protective measures to secure TGC's systems and are examining additional ones we can take to help prevent incidents of this kind in the future. In this letter, we are providing steps you may take to protect yourself against any potential misuse of your personal information.

Additionally, attached to this letter as Attachment A is a letter with the subject line "Important Confidential Security Notification and Credit Monitoring Services" ("Credit Monitoring Service Letter"). The Credit Monitoring Service Letter offers all former TGC employees a complimentary membership to Experian's IdentityWorks service with instructions on how to activate such membership. Please note that the deadline to activate such membership is November 29, 2024.

What You Can Do

We encourage you to enroll in the Credit Monitoring Services. Since your W-2 form was likely exposed, you should complete the attached IRS form 14039. Fax it to the IRS along with the identification required by the form. The fax number is (855) 807-5720. While W-2 forms for the 2023 tax year were likely exposed, if you have already filed your return for 2023 there is very little likelihood that the criminals could file a tax return in your name and interfere with any refund you were due. You should work with your tax preparer to make sure your banking information is correct, to file your returns and to follow up with the IRS regarding your refunds. The IRS has a Taxpayer Guide to Identity Theft, which we recommend you review. You can find it online at <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. Please see the FAQs attached for additional information.

You should remain vigilant for incidents of fraud and identity theft including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain free credit reports from each nationwide credit reporting agency. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the accuracy and completeness of the information in your reports. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(888) 378-4329
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
P.O. Box 955
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com

The credit reporting agencies may also allow you to view your current credit report online on a weekly basis without charge. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file.

For More Information

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Please know that TGC regrets any inconvenience or concern this incident may cause you. Please do not hesitate to contact us at **626-899-3371** if you have any questions or concerns.

Sincerely,

Janet Caldwell
Janet Caldwell
Chief Financial and Operations Officer

IF YOU ARE A CALIFORNIA RESIDENT: Even if you do not find any signs of fraud on your credit reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. The law allows you to order a free credit report from each agency every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to monitor the accuracy and completeness of the information in your reports. Just call one of the numbers above to order your report and keep the "fraud alert" in place. For more information on identity theft, you may visit the California Office of Privacy Protection website, www.oag.ca.gov/privacy.

IF YOU ARE AN INDIANA RESIDENT: For additional steps you may want to take to protect yourself please read the Indiana Identity Theft Prevention section online at www.IndianaConsumer.com for more information about situation-specific actions and responses.

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website at www.dos.ny.gov/consumerprotection.

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE A SOUTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the South Carolina Department of Consumer Affairs, 293 Greystone Boulevard, Ste. 400, Columbia, SC 29210; (803) 734-4200; <https://consumer.sc.gov/consumer-resources>



THE GILL CORPORATION

HIGH PERFORMANCE COMPOSITE PRODUCTS SINCE 1945

September __, 2024

[Name]

[Address 1]

[Address 2]

Re: Notice of Data Breach

Dear [Name]

On behalf of The Gill Corporation ("TGC") I am writing to you about a cyber-attack on TGC that occurred in late June 2024 ("Cyber-Attack"). During the Cyber-Attack an unauthorized third party compromised TGC's systems by encrypting many TGC files and backup systems. Since the Cyber-Attack, TGC has been investigating whether, among other things, the Cyber-Attack may have resulted in the unauthorized access to and the acquisition of the personal information of former TGC employees. Although TGC's investigation is ongoing, we have reason to believe that some personal information we obtained from you in the course of your employment with TGC was accessed and taken during the Cyber-Attack. This unauthorized access likely occurred on or around June 23, 2024. We are notifying you so that you may take steps to protect yourself. We take security very seriously and deeply regret that this incident occurred.

What Information was Involved?

We began investigating the incident as soon as we learned of it. Although our investigation is ongoing, we have determined that the personal information pertaining to you that may have been involved in this incident may have included your name and Social Security Number and a limited number of driver's license numbers and/or bank account numbers. Your form W-2 for past years was likely to have been exposed.

What We are Doing.

We have identified the vulnerability that was exploited by the third party and we have removed it from TGC's systems. We have already deployed additional protective measures to secure TGC's systems and are examining additional ones we can take to help prevent incidents of this kind in the future. In this letter, we are providing steps you may take to protect yourself against any potential misuse of your personal information.

Additionally, attached to this letter as Attachment A is a letter with the subject line "Important Confidential Security Notification and Credit Monitoring Services" ("Credit Monitoring Service Letter"). The Credit Monitoring Service Letter offers all former TGC employees a complimentary membership to Experian's IdentityWorks service with instructions on how to activate such membership. Please note that the deadline to activate such membership is November 29, 2024.

What You Can Do

We encourage you to enroll in the Credit Monitoring Services. Since your W-2 form was likely exposed, you should complete the attached IRS form 14039. Fax it to the IRS along with the identification required by the form. The fax number is (855) 807-5720. While W-2 forms for the 2023 tax year were likely exposed, if you have already filed your return for 2023 there is very little likelihood that the criminals could file a tax return in your name and interfere with any refund you were due. You should work with your tax preparer to make sure your banking information is correct, to file your returns and to follow up with the IRS regarding your refunds. The IRS has a Taxpayer Guide to Identity Theft, which we recommend you review. You can find it online at <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. Please see the FAQs attached for additional information.

You should remain vigilant for incidents of fraud and identity theft including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain free credit reports from each nationwide credit reporting agency. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the accuracy and completeness of the information in your reports. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(888) 378-4329
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
P.O. Box 955
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com

The credit reporting agencies may also allow you to view your current credit report online on a weekly basis without charge. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file.

For More Information

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Please know that TGC regrets any inconvenience or concern this incident may cause you. Please do not hesitate to contact us at **626-899-3371** if you have any questions or concerns.

Sincerely,

Janet Caldwell
Janet Caldwell
Chief Financial and Operations Officer

IF YOU ARE A CALIFORNIA RESIDENT: Even if you do not find any signs of fraud on your credit reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. The law allows you to order a free credit report from each agency every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to monitor the accuracy and completeness of the information in your reports. Just call one of the numbers above to order your report and keep the "fraud alert" in place. For more information on identity theft, you may visit the California Office of Privacy Protection website, www.oag.ca.gov/privacy.

IF YOU ARE AN INDIANA RESIDENT: For additional steps you may want to take to protect yourself please read the Indiana Identity Theft Prevention section online at www.IndianaConsumer.com for more information about situation-specific actions and responses.

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website at www.dos.ny.gov/consumerprotection.

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE A SOUTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the South Carolina Department of Consumer Affairs, 293 Greystone Boulevard, Ste. 400, Columbia, SC 29210; (803) 734-4200; <https://consumer.sc.gov/consumer-resources>