

BakerHostetler

Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

August 4, 2023

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

Dear Attorney General Brown:

I am writing on behalf of my client, Gunster, Yoakley & Steward, PA (“Gunster”), to notify you of a security breach involving a Maryland resident. Gunster is located at 777 South Flagler Drive, Suite 500, West Palm Beach, FL 33401.

On November 27, 2022, Gunster detected a data security incident. Gunster immediately took measures to contain the incident and securely restore its network. A thorough investigation was conducted with the assistance of firms that have helped other law firms address similar incidents. Gunster determined from the investigation that there was unauthorized access to its document management file system over the weeks leading up to the discovery of the incident. After Gunster identified the files involved, they began a process to review those files to identify the content. Gunster also notified federal law enforcement and has been in communication with them regarding the incident.

Gunster reviewed the accessed files and determined that the files contained information related to one Maryland resident, including the individual’s name and Social Security number.

On August 4, 2023, Gunster mailed a notification letter via United States Postal Service First-Class mail to the individual in Maryland whose information may have been involved in accordance with Md. Code Ann., Com. Law § 14-3504. A sample copy of the notification letter is enclosed. Gunster is offering the resident a complimentary membership to credit monitoring and identity protection services through Kroll. Gunster also has established a dedicated, toll-free call center to answer questions the individuals may have.

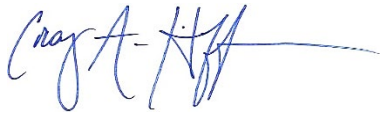
August 4, 2023

Page 2

To help prevent this type of incident from happening again, Gunster has implemented additional measures to further strengthen the security of its network.

To help prevent this type of incident from happening again, Gunster has implemented additional measures to further strengthen the security of its network. It is possible that you have received or will receive notices from certain of Gunster's clients relating to individuals to whom Gunster has sent individual notices and that are associated with this notice we are providing to you. In those situations, the individual's information came into Gunster's possession in connection with Gunster's work for the client, and the client determined to also send notice to you.

Sincerely,

A handwritten signature in blue ink, appearing to read "Craig A. Hoffman", with a long horizontal flourish extending to the right.

Craig A. Hoffman
Partner

Enclosure



<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

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

Re: Notice of Data Breach

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

Gunster, Yoakley, & Stewart, PA (Gunster) is a law firm that obtained your information in connection with the provision of legal services. We are writing to notify you of a data security incident that occurred at Gunster and involved some of your information. This notice explains the law firm's incident, measures taken to protect the information, and some steps you may consider taking in response. We regret that this incident occurred and apologize for any inconvenience.

What Happened?

Upon detecting the data security incident on November 27, 2022, we immediately took measures to contain the incident and securely restore our network. A thorough investigation was conducted with the assistance of firms that have helped other law firms address similar incidents. We determined from the investigation that there was unauthorized access to our document management file system over the weeks leading up to our discovery of the incident. After we identified the files involved, we began a process to review those files to identify the content. We also notified federal law enforcement and have been in communication with them regarding the incident.

What Information Was Involved?

Based on the review of the files involved, Gunster determined that they contained your <<b2b_text_2(name, data elements)>>.

What We Are Doing.

Gunster has implemented additional measures to further strengthen the security of its network. We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. For more information on how to help safeguard your identity and Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, please visit the below website and see the additional information provided with this letter.

What You Can Do.

For more information on your complimentary membership to Kroll identity monitoring services, as well as additional steps you can take in response to this incident, please see the pages that follow this letter.

For More Information.

If you have any questions, please call 1-866-869-0385, Monday through Friday, between 9:00 am and 6:30 pm, Eastern Time, excluding some U.S. holidays.

Enclosed: Kroll Identity Protection Enrollment Information

Additional Steps to Help Protect Yourself document

U.S. State Notification Requirements



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

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

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.

\$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.

You Can Take Additional Steps to Help Protect Yourself

Place a one-year fraud alert on your credit file

An **initial one-year fraud alert** tells anyone requesting your credit file that you might be at risk for fraud. A lender should verify that you have authorized any request to open a credit account in your name, increase the credit limit and/or get a new card on an existing account. If the lender can't verify this, they shouldn't process the request.

Contact any one of the credit reporting agencies to set up an initial one-year fraud alert.

Equifax

PO Box 105069
Atlanta, GA 30348
1-800-525-6285
equifax.com

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742
experian.com

TransUnion

PO Box 2000
Chester, PA 19016
equifax.com
1-800-680-7289
transunion.com

Place a security freeze on your credit file

A **security freeze** on your credit file prevents anyone from accessing your credit report and therefore from issuing credit in your name. **However, placing a security freeze also may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.**

Contact all three of the credit reporting agencies above to set up a security freeze with each of them.

Order your free annual credit reports

Visit annualcreditreport.com or call 1-877-322-8228 to get a free copy of your credit reports. Once you receive them:

- Verify that all information is correct.
- Look for discrepancies such as accounts you didn't open or creditor inquiries you didn't authorize.
- Contact the credit reporting agency if you notice incorrect information or have questions.

Manage your personal information

- Carry only essential documents with you.
- Be cautious about sharing your personal information with anyone else.
- Shred receipts, statements, and other documents containing sensitive information.
- Use anti-virus software on your computer and keep it updated.

Use tools to monitor your credit and financial accounts

- We suggest that you carefully review your credit reports and bank, credit card and other account information on chase.com and in statements for any transaction you don't recognize.
- We can provide copies of past statements at no cost to you.
- Call us at 1-800-392-5749 to report unauthorized transactions.
- Work with us to close your account(s) and open new ones with new account numbers.
- Create alerts with your credit card company and bank to notify you of activity.
- File an identity-theft report with your local police and contact the credit reporting agency that issued the report if you find unauthorized or suspicious activity on your credit report.

Get more information about identity theft and ways to protect yourself

- Visit experian.com/blogs/ask-experian/category/credit-advice/fraud-and-identity-theft/
- Call the Federal Trade Commission (FTC) identity theft hotline at 1-877-438-4338 (TTY: 1-866-653-4261) or visit identitytheft.gov

U.S. State Notification Requirements

For residents of California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, New Mexico, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming:		
A Summary of Your Rights Under the Fair Credit and Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer 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 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. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements carefully, monitoring your credit report for unauthorized activity and to detect errors. You may request your free annual credit report, whether or not you suspect any unauthorized activity on your account, by visiting www.AnnualCreditReport.com or calling 1-877-FACTACT (1-877-322-8228). You may also obtain a free copy of your credit report by contacting any one or more of the national consumer reporting agencies listed below. They also provide you with information about fraud alerts and security freezes.		
Equifax PO Box 740241 Atlanta, GA 30374 1-866-349-5191 equifax.com	Experian PO Box 2002 Allen, TX 75013 1-888-397-3742 experian.com	TransUnion PO Box 1000 Chester, PA 19016 1-800-888-4213 transunion.com
For residents of Iowa:		
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.		

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Attorney General and the Federal Trade Commission.

For residents of District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:

State laws require us to tell you that you can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or security freeze). If you are a District of Columbia, Maryland, New York, North Carolina or Rhode Island resident, you may also be able to obtain this information from your state's Attorney General.

Gunster, Yoakley & Stewart, P.A. is located at 600 Brickell Avenue, Suite 3500, Miami, Florida 33131. The phone number is 800-330-1980.

MD Attorney General's Office Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 oag.state.md.us	NC Attorney General's Office Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 ncdoj.gov/	Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) ftc.gov/bcp/edu/microsites/idtheft/
RI Attorney General's Office Consumer Protection Division 150 South Main Street Providence, RI 02903 1-401-274-4400 riag.ri.gov	NY Attorney General's Office Bureau of Internet and Technology 28 Liberty Street New York, NY 10005 1-212-416-8433 https://ag.ny.gov/resources/individuals/consumer-issues/technology	DC Attorney General's Office Consumer Protection 441 4 th Street, NW Washington, DC 20001 1-202-727-3400 oag.dc.gov/consumer-protection/consumer-alert-identity-theft

For residents of Connecticut, District of Columbia, New Mexico, Rhode Island, and West Virginia:

You have the right to place a security freeze on your credit report. This prohibits a credit reporting agency from releasing any information about your credit report without your written authorization. However, placing a security freeze also may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. You can place a security freeze on your credit report free of charge.

If you are the victim of identity theft, you have the right to file a police report and obtain a copy. For instructions on how to place a security freeze, visit the websites of all three major credit reporting agencies, call or write them.

When requesting a security freeze, you may need to include the following:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification

Equifax Security Freeze

PO Box 105788
Atlanta, GA 30348
1-800-349-9960
equifax.com/personal/credit-report-services/

Experian Security Freeze

PO Box 9554
Allen, TX 75013
1-888-397-3742
experian.com/freeze/center.html

TransUnion Security Freeze

PO Box 160
Woodlyn, PA 19094
1-888-909-8872
transunion.com/credit-freeze

BakerHostetler

Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

July 30, 2024

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

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

Re: Supplemental Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Gunster, Yoakley & Stewart, PA ("Gunster"), to supplement the prior notification provided to your office on August 4, 2023.

As previously summarized, on November 27, 2022, Gunster detected a data security incident. Gunster immediately took measures to contain the incident and securely restore its network. A thorough investigation was conducted with the assistance of firms that have helped other law firms address similar incidents. Gunster determined from the investigation that there was unauthorized access to its document management file system over the weeks leading up to the discovery of the incident. After Gunster identified the files involved, they began a process to review those files to identify the content. Gunster also notified federal law enforcement and has been in communication with them regarding the incident.

Based on that review, Gunster began mailing notifications to individuals in April 2023 and, on August 4, 2023, provided substitute notice via nationwide media and a post on Gunster's website. The file review continued, and, on October 15, 2023, the review process generated a preliminary list of individuals whose information was contained in the files. Gunster then worked to review the list and supplement it with addresses and other information to be able to identify individuals to notify. The review confirmed that the files contained information related to Maryland residents, including the individuals' name and one or more of the following data elements: Social Security number, driver's license number, passport or other government identification number, financial

July 30, 2024

Page 2

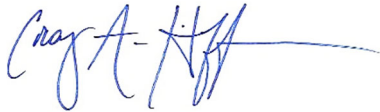
account number, payment card number, medical treatment information, health insurance information, username and password, and/or email address and password.

Gunster conducted an additional mailing on December 1 and 4, 2023. Gunster's review continued and notification letters were mailed on a rolling basis as individuals were identified and addresses were confirmed. The data review and notification process is now complete. Approximately 4,303 Maryland residents were notified.

Gunster is offering the residents a complimentary membership to credit monitoring and identity protection services through Kroll. Gunster also has established a dedicated, toll-free call center to answer questions the individuals may have.

To help prevent this type of incident from happening again, Gunster has implemented additional measures to further strengthen the security of its network.

Sincerely,

A handwritten signature in blue ink, appearing to read "Craig A. Hoffman", with a long horizontal flourish extending to the right.

Craig A. Hoffman
Partner