<u>Chicago District Golf Association Notice of Data Security Incident</u>

[www.cdga.org] Chicago District Golf Association ("CDGA") has become aware of a data security Incident that may have resulted in an unauthorized access to your sensitive personal information. CDGA sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

<u>What Happened?</u> On September 7, 2023, CDGA learned they were the victim of a cybersecurity incident. Upon discovery of this Incident, CDGA promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. CDGA is still analyzing the results of the forensic investigation; however, out of full transparency, CDGA is providing notice about the potential access to sensitive information by an unauthorized actor. CDGA is working to identify all the specific individuals and the type of data that was potentially accessed in order to provide sufficient notice to individuals. CDGA will mail formal notice letters to those impacted individuals once they are identified.

<u>What Information Was Involved</u>? The investigation is still ongoing. However, if sensitive information is found to have been potentially compromised, a formal notice letter will be sent to those who have had their sensitive information impacted, and the letter will identify the types of information involved.

<u>What We Are Doing</u>. CDGA is committed to ensuring the privacy and security of all personal information in our care. Since the discovery of the Incident, CDGA has taken and will continue to take steps to mitigate the risk of future issues. Specifically, CDGA *has engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. Also, additional security practices have been implemented that include retraining employees, updating policies, and implementing a weekly security scan of the site to determine if there are any issues.*

If there was unauthorized access to sensitive information, CDGA will be offering complimentary credit monitoring and identity theft protection services to those impacted individuals. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. CDGA strongly encourages all identified individuals to register for this free service.

<u>What You Can Do</u>. CDGA encourages all members to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that individuals contact his/her financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect his/her interests, including the possible placement of a fraud alert on the credit file.

<u>For More Information</u>. CDGA recognizes that our members may have questions not addressed in this notice. For more information, *please send an e-mail with your questions to notice@cdga.org. We will respond as soon as possible.*

Sincerely,
CDGA Inc.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

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 *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 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 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 violators. 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 at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. **Federal Trade Commission -** Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-9995630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - you may also may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

New York Office of Attorney General - 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 Office of the Attorney General - the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1401-274-4400**;** www.riag.ri.gov.

June 4, 2024

Brian H. Myers
(202) 626-7695 (direct)
Brian.Myers@WilsonElser.com

Via Email:

Office of the Attorney General
Attn: Security Breach Notifcation
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Update to Notice of Cybersecurity Incident Involving Chicago District Golf Association

Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Chicago District Golf Association ("CDGA"), located at 11855 Archer Avenue in Lemont, Illinois 60439, and we are providing this update to our April 19, 2024 notice of a recent cybersecurity incident (hereinafter, the "Incident"). By providing this notice, CDGA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

This letter will serve to inform you of the nature of the Incident, what information may have been affected, and the steps that CDGA has taken in response to the Incident. We have also enclosed hereto a sample copy of the notice letter we recently mailed to the affected individuals on May 31, 2024.

1. Nature of the Incident

On September 7, 2023, CDGA was alerted to suspicious credit card activity involving users of its website. CDGA immediately coordinated with its third-party payment card processor to engage cybersecurity professionals to conduct a forensic investigation.

On January 2, 2024, while CDGA's investigation was ongoing, CDGA posted a preliminary notice of the incident on its website.

On March 26, 2024, CDGA's third-party cybersecurity experts concluded their investigation and found that an unauthorized actor installed malicious software on CDGA's website and deployed advanced techniques to evade detection. CDGA has eliminated the malicious software and secured its website.

Based on these findings, CDGA reviewed the affected systems to identify and notify any individuals whose personal information may have been affected. On April 19, 2024, While CDGA's review was ongoing, CDGA provided a preliminary notice to this office.

CDGA recently completed its review and on May 31, 2024, CDGA mailed personalized notification letters to the affected individuals.

2. Number of individuals and information involved.

CDGA's investigation determined that the personal information of three (3) Maryland residents was affected. For each individual, the categories of personal information involved included their names and credit card information.

3. Steps taken in response to the Incident.

Data privacy and security is among CDGA's highest priorities. Upon discovery of the Incident, CDGA moved quickly to investigate and respond to the Incident and assess the security of its systems. Specifically, CDGA engaged specialized cybersecurity professionals to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, CDGA took the following steps, including, but not limited to: implementing new technical safeguards; revised policies and procedures; and enhanced monitoring, detection, and reporting.

In addition, the personalized notification letters that CDGA mailed on May 31, 2024 included an offer of complimentary credit monitoring and identity theft protection services, along with instructions on how to enroll in those services.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at Brian.Myers@WilsonElser.com or (202) 626-7695.

Regards,

Wilson Elser Moskowitz Edelman & Dicker LLP

Brian H. Myers, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.

Cyberscout
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Via First-Class Mail
P
[redacted]

000010102G0500

P

May 28, 2024

Dear [redacted]:

Chicago District Golf Association ("CDGA") is writing to inform you of a data security incident that potentially involved your personal information. We are providing you with information about the incident, steps we are taking in response, and resources you can use to help protect against the potential misuse of your data. Please be assured CDGA takes the protection of your data seriously.

What Happened

On September 7, 2023, CDGA was alerted to suspicious credit card activity involving users of its website. CDGA immediately coordinated with its third-party payment card processor and engaged cybersecurity professionals to conduct a forensic investigation into the nature and scope of the incident. While our investigation was ongoing, on January 2, 2024, we posted a preliminary notice of the incident on our website.

On March 26, 2024, CDGA's third-party cybersecurity experts concluded their investigation and found that an unauthorized actor installed malicious software on CDGA's website and deployed advanced techniques to evade detection. CDGA has eliminated the malicious software and secured its website.

What Information Was Involved

Based on the investigation, the following categories of your personal information may have been affected: credit card information

What We Are Doing

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to engage leading cybersecurity professionals to conduct a forensic investigation and secure our network. We eliminated the malicious software, deployed new technical safeguards, revised our policies and procedures, and enhanced our network monitoring, detection, and reporting solutions.

As part of our ongoing commitment to the security of your personal information, we are offering you 12 months of **free credit monitoring and identity theft protection services**. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Please review the enclosed *Additional Information About Identity Theft Protection* to learn more about how to protect against the possibility of any misuse of your personal information.

You can also enroll in the Credit Monitoring services that we are offering at no cost to you. Please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided to enroll. When prompted please provide the following unique code to receive services: [redacted]**.** Please note that the code is case-sensitive and will need to be entered as it appears.

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have [redacted] months of monitoring services. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

We take this incident and the security of personal information in our care seriously. If you have additional questions, representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line 833-566-5948 and provide the representative with the unique code listed above. The call center representatives can answer questions or concerns you may have regarding the protection of your personal information.

Jack Childers

Jack Childers
President
Chicago District Golf Association

Additional Information About Identity Theft Protection

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-349-9960	1-888-397-3742	1-888-909-8872
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:
- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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.

P 00001020280000

Please note that in order 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. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the 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.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 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 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 violators. 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 at 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, 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

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents: 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. This incident involved the personal information of one Rhode Island resident. 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.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

June 4, 2024

Brian H. Myers
(202) 626-7695 (direct)
Brian.Myers@WilsonElser.com

Via Email:

Office of the Attorney General
Attn: Security Breach Notifcation
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Update to Notice of Cybersecurity Incident Involving Chicago District Golf Association

Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Chicago District Golf Association ("CDGA"), located at 11855 Archer Avenue in Lemont, Illinois 60439, and we are providing this update to our April 19, 2024 notice of a recent cybersecurity incident (hereinafter, the "Incident"). By providing this notice, CDGA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

This letter will serve to inform you of the nature of the Incident, what information may have been affected, and the steps that CDGA has taken in response to the Incident. We have also enclosed hereto a sample copy of the notice letter we recently mailed to the affected individuals on May 31, 2024.

1. Nature of the Incident

On September 7, 2023, CDGA was alerted to suspicious credit card activity involving users of its website. CDGA immediately coordinated with its third-party payment card processor to engage cybersecurity professionals to conduct a forensic investigation.

On January 2, 2024, while CDGA's investigation was ongoing, CDGA posted a preliminary notice of the incident on its website.

On March 26, 2024, CDGA's third-party cybersecurity experts concluded their investigation and found that an unauthorized actor installed malicious software on CDGA's website and deployed advanced techniques to evade detection. CDGA has eliminated the malicious software and secured its website.

Based on these findings, CDGA reviewed the affected systems to identify and notify any individuals whose personal information may have been affected. On April 19, 2024, While CDGA's review was ongoing, CDGA provided a preliminary notice to this office.

CDGA recently completed its review and on May 31, 2024, CDGA mailed personalized notification letters to the affected individuals.

2. Number of individuals and information involved.

CDGA's investigation determined that the personal information of three (3) Maryland residents was affected. For each individual, the categories of personal information involved included their names and credit card information.

3. Steps taken in response to the Incident.

Data privacy and security is among CDGA's highest priorities. Upon discovery of the Incident, CDGA moved quickly to investigate and respond to the Incident and assess the security of its systems. Specifically, CDGA engaged specialized cybersecurity professionals to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, CDGA took the following steps, including, but not limited to: implementing new technical safeguards; revised policies and procedures; and enhanced monitoring, detection, and reporting.

In addition, the personalized notification letters that CDGA mailed on May 31, 2024 included an offer of complimentary credit monitoring and identity theft protection services, along with instructions on how to enroll in those services.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at Brian.Myers@WilsonElser.com or (202) 626-7695.

Regards,

Wilson Elser Moskowitz Edelman & Dicker LLP

Brian H. Myers, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.