

February 27, 2023

Via Email: IDtheft@oag.state.md.us



801 Mount Vernon Place NW
Washington, DC 20001

P: 202.249.3000
F: 202.249.3255

eventsdc.com

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

To Whom it May Concern:

This letter serves as notice that the Washington Convention and Sports Authority t/a Events DC ("Events DC") experienced a data security incident. Specifically, on September 29, 2022, Events DC discovered and confirmed that system files and information were encrypted by an unknown threat actor employing what is believed to have been the Black Cat/ALPHV malware variant. Events DC moved quickly to contain the intrusion, immediately engaged a leading cyber security forensics consultant, and notified federal law enforcement. A general description of the incident and the remedial measures taken are provided in the attached notice to be sent to the 538 affected Maryland residents.

Your office is welcome to contact me at njackson@eventsdc.com or (202) 249-3216 or Deputy General Counsel Reginald L. Smith at rsmith@eventsdc.com or (202) 249-3224 if you require additional information.

Sincerely,

A handwritten signature in blue ink, appearing to read "Nicole B. Jackson".

Nicole B. Jackson
General Counsel

cc: Reginald L. Smith
Vice President and Deputy General Counsel
Events DC

Attachment

[Individual's name]
[Individual's address]
[City, State, Zip]

[Date]

Dear [_____]:

Notice of Cybersecurity Incident

Events DC takes the protection of your personal information very seriously. We write to notify you of an incident that may have involved some of that information. Please read this notice carefully, as it provides information about the incident, the personal information that may have been involved, the steps we are taking to ensure the security of our systems, and the resources available to you to protect yourself against any unauthorized use of your personal information. We have included the telephone number for our dedicated assistance line and our contact information below should you need any further information.

What Happened?

On September 29, 2022, Events DC discovered that we were the victim of a cyberattack on parts of our network. As a result, and as we told you by email on October 28, 2022, there is reason to believe that some sensitive employee information was compromised. We have been working in close collaboration with external cyber forensics experts and the appropriate authorities to thoroughly investigate the incident and secure our systems. Our top priority throughout this situation has been our employees, customers, and stakeholders.

What Information Was Involved?

You are receiving this notice because our review determined that the cyberattack may have resulted in unauthorized access and acquisition of one or more files containing your name, address, phone number, email address, date of birth, Social Security number, medical information, and/or limited information regarding your choice of health insurance and other benefits. The fact that you are receiving this notice does not mean that all or more than one of the aforementioned files and information relating to your personal information were actually acquired.

What We Are Doing

Because the protection of your privacy is so important to us, we have taken several steps to further fortify our systems and detect suspicious activity on our networks. While we have no indication that your information has been used to commit fraud or identity theft, and as we told you by email on October 28, 2022 (and in a follow-up reminder email on December 19, 2022), we offered you free credit monitoring and identify theft protection through a 12-month subscription to Legal Resources Platinum Identity Protection. We are now offering you a total of 18 months subscription to Legal Resources Platinum Identity Protection. If you originally enrolled in a 12-month subscription, it has been automatically extended for an additional six months and there is nothing

more you need to do. This product provides you and any impacted family members with full-service identity detection and resolution of identity theft. You were granted immediate access to their website, support team and overview of applicable benefits. Please refer to the October 28th email sent by Legal Resources to your Events DC email account for complete membership details. If you were unable to activate your account, please call Legal Resources' customer care team at 800-728-5768.

What You Can Do

We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment cards and personal accounts for unauthorized charges and be sure to monitor free credit reports for fraudulent or unusual activity. If you suspect an unauthorized charge has been placed on your account, report it to your payment card issuer immediately. According to the payment card brands' policies, you are not responsible for unauthorized charges to your account if you report them in a timely manner.

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, 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, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

For More Information

You may contact our dedicated assistance line with questions and concerns by calling (833) 514-1445 toll-free Monday through Friday from 8 am - 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **B085795**. You may also mail us a letter at Events DC, 801 Mount Vernon Place NW, Washington, DC 20001, or call our general company phone line at 202-249-3000.

Sincerely,

A handwritten signature in blue ink that reads "Angie M. Gates". The signature is fluid and cursive, with the first name "Angie" being the most prominent part.

Angie M. Gates
President and Chief Executive Officer
Events DC

ADDITIONAL STEPS YOU CAN TAKE

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. You should 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 and your state attorney general is as follows:

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

State Attorney General:

For DC residents: *District of Columbia Office of the Attorney General*, 400 6th Street NW, Washington, DC 20001, 202-727-3400, <https://oag.dc.gov/>

For Maryland residents: *Maryland Office of the Attorney General*, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For North Carolina residents: *North Carolina Office of the Attorney General*, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7266, www.ncdoj.gov

For Virginia residents: *Virginia Office of the Attorney General*, 202 North Ninth Street, Richmond, Virginia 23219, 804-786-2071, <https://www.oag.state.va.us>

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, please 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 a creditor 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, please contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

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

You will 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 time by lifting the freeze only at that particular credit bureau. Otherwise, you will need to make the request with all three credit bureaus.

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 N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.

- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.