

Holland & Knight

31 West 52nd Street | New York, NY 10019 | T 212.513.3200 | F 212.385.9010
Holland & Knight LLP | www.hklaw.com

Mark H. Francis
+1 212-513-3572
Mark.Francis@hklaw.com

May 23, 2022

VIA E-MAIL TO IDTHEFT@OAG.STATE.MD.US

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

Re: Notice of Security Incident

To Whom it May Concern:

I am writing on behalf of A.D. Starr (a Dick's Sporting Goods, Inc. business), to inform you that notice is being sent to approximately 83 Maryland residents regarding a security incident that potentially impacted credit card information submitted to the adstarr.com website due to malicious software found in the payment processing functionality of a third-party vendor, Freestyle Solutions, Inc. ("Freestyle"). This incident was limited to A.D. Starr's website and did not impact any business affiliate or parent of A.D. Starr.

- I. Nature of the Security Incident.** In early February 2022, Freestyle became aware of malicious software running on the payment processing server operated for another company, and after further investigation it found similar issues on servers maintained for other customers, including A.D. Starr. Freestyle immediately blocked the malicious software and retained outside data security experts to conduct a forensic investigation of the incident. Freestyle reported the incident to major card brands (VISA, MasterCard, etc.) so they can be on heightened alert for potential fraud on impacted cards. The investigation by Freestyle's outside data security experts is still ongoing, in coordination with the card brands. Freestyle also reported the incident to federal law enforcement authorities. A.D. Starr is currently awaiting Freestyle's investigation findings and reviewing the security safeguards implemented for its website.
- II. Type of Information Compromised.** Payment card information submitted on adstarr.com between September 18, 2020 and February 3, 2022 may have been acquired by an unauthorized party. Specifically, the malicious software may have obtained cardholder name, payment card number, card verification code and expiration date for approximately 3,200 customers. Freestyle found no evidence that other personal information was impacted.
- III. Number of Residents Affected and Notified.** Notice to potentially affected individuals is being sent via USPS mail on May 23, 2022. A.D. Starr arranged with Experian to offer all noticed individuals a free year of active credit monitoring and, if needed, identity theft assistance and insurance. A.D. Starr also provided a detailed explanation of additional steps that potentially-affected individuals may consider taking, free of charge, to further protect themselves, including checking credit reports, utilizing fraud alert services and placing a security freeze on credit reports. Please see the enclosed copy of the template notification letter for additional details. Notification was not delayed due to a law enforcement investigation.

Office of the Attorney General
May 23, 2022

Please contact me if you have any questions.

Sincerely yours,

s/ Mark Francis

Mark H. Francis
Holland & Knight LLP

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 23, 2022

H9145-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Important Security Notification

Dear Sample A. Sample,

A.D. Starr recently became aware of a security incident that potentially impacted credit card information submitted to our adstarr.com website due to malicious software found in the payment processing functionality of our vendor. This incident is strictly limited to A.D. Starr's website and did not impact any business affiliate or parent of A.D. Starr. We are reaching out to provide notice of this incident and how we are responding, as well as offer free credit monitoring and steps that you can take to protect your information.

What Happened? In early February 2022, a vendor that A.D. Starr uses became aware of malicious software running on the payment processing server operated for another company, and after further investigation it found similar issues on servers maintained for other customers, including A.D. Starr. The vendor immediately blocked the malicious software and retained outside data security experts to conduct a forensic investigation of the incident.

What Information Was Impacted? Payment card information submitted on adstarr.com between September 18, 2020 and February 3, 2022 may have been acquired by an unauthorized party. Specifically, the malicious software may have obtained cardholder name, payment card number, card verification code and expiration date. The vendor found no evidence that other personal information was impacted.

What Are We Doing? The vendor reported the incident to major card brands (VISA, MasterCard, etc.) so they can be on heightened alert for potential fraud on impacted cards. The investigation by the vendor's outside data security experts is still ongoing, in coordination with the card brands. The vendor also reported the incident to federal law enforcement authorities. The payment processing functions of the A.D. Starr website have been subject to a thorough security review to ensure the malicious software was removed, and operations have resumed without issue. A.D. Starr is actively engaged with the vendor as the investigation comes to a close to make sure all findings are reviewed and any necessary additional security safeguards are implemented for the payment processing functions of the website.

What Can You Do? We encourage you to remain vigilant by reviewing your account statements and contacting your financial institution or card issuer immediately if you believe there is an unauthorized charge on your card. Card brand policies generally provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. The following sections provide additional steps you can take to protect your personal information.

0000001



H9145-L01

Free Credit Monitoring Offer. To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM, including both identity detection services and assistance in the event of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: **August 31, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: **ABCDEFGHI**

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 **(833) 637-2105** by **August 31, 2022**. Be prepared to provide engagement number **B053539** as proof of eligibility for the identity restoration services by Experian.

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.¹
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration agents 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.²
- Up to \$1 Million Identity Theft Insurance³: 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 (833) 637-2105. 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). Identity Restoration support is available to you for one year 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.

Additional resources for protecting your personal information. (1) *Getting a credit report*. Under U.S. law, individuals over the age of 18 are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the credit bureaus directly to request a free copy of their credit report.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² Even after the 1-year monitoring services expire, enrollees may still contact Experian to receive Identity Restoration assistance.

³ Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

(2) *Placing a fraud alert.* If you believe you are at risk of identity theft, you can have the credit bureaus place a “fraud alert” on your credit file that alerts creditors to take additional steps prior to granting credit in your name. Note, however, that this may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts as well. To place a fraud alert or inquire about your credit report, you can contact the credit reporting agencies using the information below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-680-7289
www.transunion.com

(3) *Placing a security freeze.* You can also place a “security freeze” on your credit reports. This prohibits a credit reporting agency from releasing information from your credit report without your authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests they make for new loans, credit mortgages, employment, housing, or other services. You cannot be charged to place or lift a security freeze on your credit report. A security freeze needs to be separately requested with each of the credit bureaus, and you may need to supply certain personal information in order to confirm your identity when making the request. To find out more about security freezes, you can contact the credit reporting agencies using the information below:

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

(4) *Learning more about identity theft.* You can learn more about identity theft, fraud alerts, and steps you can take to protect yourself by contacting the Federal Trade Commission (FTC) or state Attorney General. The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint with them, and you can do so at www.identifytheft.gov. Identity theft should also be reported to your local law enforcement.

(5) *State-specific information.* **For Kentucky residents:** The Office of the Attorney General of Kentucky can be contacted at, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601; www.ag.ky.gov; or 1-502-696-5300. **For Iowa Residents:** You may report suspected incidents of identity theft to local law enforcement or to the Iowa Attorney General’s Office to at Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5164; www.iowaattorneygeneral.gov. **For Maryland Residents:** You can obtain information about steps you can take to avoid identity theft by contacting the Attorney General at Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland) or (410) 576-6300, www.marylandattorneygeneral.gov; **For New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act that include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov; **For New York Residents:** You can obtain information about how to protect yourself from identity theft and tips on how to protect your privacy online by contacting the Office of the Attorney General, The Capitol, Albany, NY 12224-



0341, 1-800-771-7755 (toll-free) or 1-800-788-9898 (TDD/TTY toll-free line), <https://ag.ny.gov/> or by contacting the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, <https://ag.ny.gov/internet/resource-center/>; **For North Carolina Residents:** You can obtain information about preventing identity theft by contacting the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdog.gov; **For Oregon Residents:** You are encouraged to report suspected identity theft to the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400, www.doj.state.or.us; **For Rhode Island Residents:** You may obtain information about preventing and avoiding identity theft by contacting the Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov. You have the right to obtain a police report and request a security freeze as described above. Consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account; **For Washington, D.C. Residents:** You may obtain information about preventing and avoiding identity theft by contacting the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov.

* * *

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions, please contact the Experian customer care team at (833) 637-2105 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 B053539.

A.D. Starr
4300 McClaren Woods Drive
Coraopolis, PA 15108