



January 26, 2023

VIA EMAIL [IDTHEFT@OAG.STATE.MD.US]

Lori Kalani

Direct Phone 202-471-3407

Direct Fax 202-618-4825

lkalani@cozen.com

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

Re: DraftKings Inc. Credential Stuffing Attacks

To Whom It May Concern:

[REDACTED]
[REDACTED] this letter is to notify you that DraftKings Inc. recently discovered potential credential stuffing attacks. [REDACTED]

[REDACTED] This notice does not constitute an admission that these credential stuffing attacks are subject to the notification provisions of the Maryland Personal Information Protection Act, Md. Code, Com. L. § 14-3501 *et seq.*, nor is this a notice of any kind of data breach of DraftKings. Rather, we are providing this formal notice at the request of your office.

DraftKings recently identified suspicious logins to certain DraftKings accounts indicative of credential stuffing attacks. "Credential stuffing attacks" are a specific type of cybersecurity attack in which bad actors use login credentials (e.g., email addresses/username and passwords) obtained from a third-party source to gain access to user accounts. Credential stuffing attacks often occur when individuals use the same login credentials on multiple websites, which is why DraftKings encourages users to use a unique password for their DraftKings account.

Based on DraftKings' review to date, it believes that attackers may have previously gained access to account usernames or email addresses and passwords from a non-DraftKings source and then used those credentials to access certain DraftKings accounts. Upon discovery of the initial credential stuffing attacks beginning on November 18, 2022, DraftKings, among other things, promptly reviewed and took a number of steps, described below. In the course of these attacks, a limited number of users may have had funds improperly withdrawn from their accounts. DraftKings has restored amounts that were withdrawn from certain accounts as determined and identified by DraftKings.

DraftKings' review to date has uncovered no evidence that these login credentials were obtained from DraftKings. However, by obtaining login credentials from a non-DraftKings source and using them in these attacks, bad actors may have been able to log into certain DraftKings accounts. In the event an account was accessed, among other things, the attacker could have viewed the account holder's name, address, phone number, email address, last four digits of

payment card, profile photo, information about prior transactions, account balance, and last date of password change. As it relates to these credential stuffing attacks discovered beginning on November 18, 2022, DraftKings has identified 3,293 potentially improper logins into Maryland user accounts.

At this time, there is currently no evidence that the attackers accessed users' Social Security numbers, driver's license numbers or financial account numbers. While bad actors may have viewed the last four digits of users' payment cards, the full payment card number, expiration date, and CVV are not stored in user accounts. Therefore, the bad actors were not able to view this information.

DraftKings promptly took steps to address these attacks including, among other things, initiating an internal review, requiring affected customers to reset their DraftKings passwords and implementing additional fraud alerts. DraftKings has restored amounts that have been withdrawn from certain accounts in connection with credential stuffing attacks, as determined and identified by DraftKings.

Attached for your reference is a sample of the notice to the affected individuals, which we will send via email on January 27, 2023. Please do not hesitate to contact me if you have any questions.

Sincerely,

COZEN O'CONNOR

A handwritten signature in cursive script that reads "Lori Kalani".

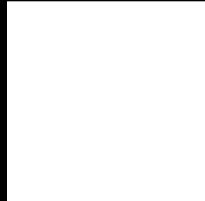
By: Lori Kalani

LK

cc: Hanna Abrams, Esq. (via email [habrams@oag.state.md.us])

Enclosure

From: DraftKings <donotreply@account.draftkings.com>
Sent: Friday, January 27, 2023 1:00 PM
To: <user email>
Subject: DraftKings Notice of Potential Credential Stuffing Incident



[USER],

DraftKings Inc. ("DraftKings") writes to follow up on our previous email sent to you notifying you of a potential incident involving your DraftKings account and directing you to reset your account password. We provide this notice to offer additional information concerning the incident and to inform you of some steps you can take to better protect yourself.

What Happened?

We recently identified suspicious logins to certain DraftKings accounts indicative of credential stuffing attacks. "Credential stuffing attacks" are a specific type of cybersecurity attack in which bad actors use login credentials (e.g., email addresses/usernames and passwords) obtained from a third-party source to gain access to user accounts. Credential stuffing attacks often occur when individuals use the same login credentials on multiple websites, which is why we encourage you to use a unique password for your DraftKings account.

Based on our investigation to date, we believe that attackers may have previously gained access to your username or email address and password from a non-DraftKings source and then used those credentials to access your DraftKings account. Upon discovery of these incidents, DraftKings, among other things, promptly investigated and took a number of steps, described below. In the course of these attacks, a limited number of users may have had funds improperly withdrawn from their accounts. We have restored amounts that were withdrawn from certain accounts as determined and identified by DraftKings.

What Information Was Involved?

Our investigation to date has uncovered no evidence that your login credentials were obtained from DraftKings. However, by obtaining login credentials from a non-DraftKings source and using them in these attacks, bad actors may have been able to log into certain DraftKings accounts. In the event an account was accessed, among other things, the attacker could have viewed the account holder's name, address, phone number, email address, last four digits of payment card, profile photo, information about prior transactions, account balance, and last date of password change.

At this time, there is currently no evidence that the attackers accessed your Social Security number, driver's license number or financial account number. While bad actors may have viewed the last four

digits of your payment card, your full payment card number, its expiration date, and its CVV are not stored in your account. Therefore, the bad actors were not able to view this information.

What We Are Doing

We promptly took steps to address these incidents including, among other things, initiating an internal investigation, requiring affected customers to reset their DraftKings passwords and implementing additional fraud alerts. We have restored amounts that have been withdrawn from certain accounts in connection with credential stuffing attacks, as determined and identified by DraftKings. We have also notified certain law enforcement and we intend to assist them.

What You Can Do

We want to make you aware of steps that you can take as a precaution:

- **Change Account Passwords.** If you haven't done so already, please use the following link to reset your DraftKings password as soon as possible: <https://www.draftkings.com/account/resetpassword>. If you use the same or similar passwords with other online accounts, we recommend that you immediately change your password for those accounts as well. You should use different and strong passwords for all accounts/websites. Tips on creating a strong password are available at <http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/>.
- **Review Accounts and Credit Reports:** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft. The FTC can be reached at: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, consumer@oag.state.md.us.

- **Security Freezes and Fraud Alerts:** 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely

approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the following national credit reporting agencies:

National Credit Reporting Agencies Contact Information

Equifax
(www.equifax.com):
General Contact:
P.O. Box 740241,
Atlanta, GA 30374
800-685-1111
**Fraud Alerts and
Security Freezes:**
P.O. Box 740256,
Atlanta, GA 30374

Experian
(www.experian.com):
General Contact:
P.O. Box 2104, Allen,
TX 75013
888-397-3742
**Fraud Alerts and
Security Freezes:**
P.O. Box 9556, Allen,
TX 75013

TransUnion
(www.transunion.com):
**General Contact, Fraud
Alerts and Security
Freezes:**
P.O. Box 2000, Chester,
PA 19022
800-916-8800

For More Information

If you have any further questions regarding this incident, or to report a suspected unauthorized withdrawal on your account, please call our dedicated and toll-free response line that we have set up to respond to questions at 1-888-397-0035 between the hours of 9am – 11pm Eastern, Monday through Friday, and 11am – 8pm Eastern, Saturday and Sunday. Please be prepared to reference engagement B084524 when speaking with an agent.

Please do not respond to this email, as this email notification is unable to receive replies. Please contact us directly at the number provided in the email above.

Sincerely,
DraftKings Inc.

DRAFTKINGS

222 Berkeley Street, Boston, MA 02116 United States



[DFS](#) | [Sportsbook](#) | [Casino](#) | [Marketplace](#)

DraftKings Inc. is a US-based company. DraftKings' Sportsbook and Casino products are regulated by the New Jersey Division of Gaming Enforcement as an internet gaming operator in accordance with the Casino Control Act N.J.S.A. 5:12-1 and its implementing regulations. Our Sportsbook and Casino games are tested by the New Jersey Division of Gaming Enforcement to provide games that are fair and operate correctly. Only customers 21 and over are permitted to play our Sportsbook and Casino games. Subject to regulatory licensing requirements.

DraftKings Inc. is a US-based company. DFS statistics are licensed from STATS LLC.

© DraftKings All Rights Reserved

This email was sent to:

This email was sent by: DraftKings Inc.

[Privacy Policies](#)

[Daily Fantasy Sports](#) | [Sportsbook/Casino](#)

To manage your DraftKings email preferences or unsubscribe, click [here](#)

