CONSTANGY
BROOKS, SMITH & PROPHETE LLP

Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067

April 27, 2023

VIA EMAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith and Prophete, LLP ("Constangy") represents Florida State Fair Authority ("FSFA") in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

On November 9, 2022, FSFA learned of unusual activity involving certain systems in its network environment. In response, FSFA immediately took steps to secure its network and engaged third-party digital forensics experts to assist with the investigation and determine whether sensitive information may have been accessed or acquired during the incident. Through the investigation, FSFA found that certain systems may have been accessed without authorization. Following this confirmation, FSFA engaged a vendor to conduct a comprehensive review of the potentially affected data and on March 22, 2023, FSFA determined that personal information belonging to certain individuals may have been impacted in connection with this incident. FSFA then worked diligently to obtain contact information to effectuate notification to potentially affected individuals. This process was completed on April 20, 2023.

FSFA is notifying all potentially impacted individuals of the incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

Please note that we have no current evidence to suggest misuse or attempted misuse of any personal information in conjunction with this incident.

2. **Number of New Hampshire residents affected.**

FSFA notified a single (1) New Hampshire resident of this incident via first class U.S. mail on April 27, 2023. The information involved in the incident may differ depending on the individual but may include the following for affected New Hampshire resident: name and Social Security number.

A sample copy of the notification letter is included with this correspondence.

Steps taken relating to the Incident.

As soon as FSFA discovered this incident, FSFA took steps to secure its network environment and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. FSFA has also implemented additional safeguards to help ensure the security of its network environment and to reduce the risk of a similar incident in the future.

FSFA has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-800-939-4170 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). In addition, while FSFA is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, FSFA is also providing complimentary identity protection services to notified individuals.

3. Contact information.

FSFA remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

Jason S. Cherry of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

4145 SW Watson Ave.
Suite 400
Beaverton, OR 97005

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 27, 2023

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Florida State Fair Authority ("FSFA") is writing to inform you of a data security incident that may have involved your personal information. We take the privacy and security of all personal information within our possession very seriously. Therefore, we are writing to inform you about the incident and advise you of certain steps you can take to help protect your personal information, including activating the free credit and identity protection services that we are offering you.

What Happened? On November 9, 2022, FSFA learned of unusual activity involving certain systems in our network. Upon discovering this activity, we immediately took steps to secure our network and engaged third-party digital forensics experts to assist with the investigation and determine whether sensitive information may have been accessed or acquired during the incident. Through the investigation, we found that certain systems may have been accessed without authorization. Following this confirmation, FSFA engaged a vendor to conduct a comprehensive review of the potentially affected data and on March 22, 2023, we determined that personal information belonging to certain individuals may have been impacted in connection with this incident. We then worked diligently to obtain contact information to effectuate notification to potentially affected individuals. This process was completed on April 20, 2023.

Although we have no evidence of the misuse or attempted misuse of any potentially impacted information, out of an abundance of caution, we are notifying you about the incident and providing complimentary credit monitoring and identity theft protection services to you.

What Information Was Involved? The potentially affected information includes your name and your <<Variable Data 1: Data Elements>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our network environment and to reduce the risk of a similar incident occurring in the future.

Additionally, to help relieve concerns and to help protect your identity following this incident, FSFA is offering you complimentary credit monitoring and identity protection services through IDX, a data breach and recovery services expert. These services include <<12/24>> months of credit[1] and dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Additional information describing the IDX services is included with this letter.

[1] To receive credit monitoring 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.

What Can You Do? Please read the recommendations included with this letter which you can follow to help protect your personal information. FSFA also encourages you to enroll in the identity protection services being offered to you, at no cost, through IDX. To enroll, please visit the IDX website at https://app.idx.us/account-creation/protect and provide your enrollment code located at the top of this page. The deadline to enroll in these services is July 27, 2023.

For More Information: If you have questions or need assistance, please contact IDX at 1-800-939-4170, Monday through Friday from 8:00 am to 8:00 pm Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Cheryl F. Flood
Executive Director
Florida State Fair Authority

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. 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 is as follows:

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

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN/password in a safe place as you will need it if you choose to lift the 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 via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504 cfpb summary your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-6268800; https://www.maine.gov/ag/

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-6210508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov