FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
321 NORTH CLARK STREET
CHICAGO, IL 60654-5313
312.832.4500 TEL
312.832.4700 FAX
WWW.FOLEY.COM

atantleff@foley.com
312.832.4367

CLIENT/MATTER NUMBER
134016-0103#

March 28, 2024

VIA E-MAIL (idtheft@oag.state.md.us)

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, Maryland 21202

Re: Notification Pursuant to Md. Code Ann., Com. Law § 14-3504

Dear Office of the Attorney General:

We are writing on behalf of our client, The Chicago Bears Football Club, Inc. (the "Bears"), to notify you of an incident involving the personal information of one (1) Maryland resident.

NATURE OF THE INCIDENT

On February 14, 2024, the Bears were alerted to suspicious activity associated with one of its employee's email accounts and immediately stopped that activity from continuing while it was still in progress. Upon becoming aware of this situation, the Bears immediately secured the account and launched an investigation. The investigation determined that an unauthorized third-party accessed the employee's email account on February 14, 2024 and may have viewed certain data stored in the account during that time.

As part of this investigation, the Bears initiated a detailed review of the emails and attachments in the affected email account to identify whether personal information belonging to individuals may have been accessible to the unauthorized party. The Bears' review concluded on February 29, 2024, at which time it determined that certain personal information of current and former players and employees of the Bears was contained within the impacted account at the time of the incident, including the full name, medical condition/diagnosis, and injury-related details associated with one (1) Maryland resident.

STEPS TAKEN IN RESPONSE TO THE INCIDENT

Although there is no evidence of actual misuse of any of this information, the Bears are notifying this resident out of an abundance of caution. The Bears will mail a notification letter to the potentially affected Maryland resident on March 28, 2024. Enclosed is a sample copy of the notice that was sent to the individual. In addition, the Bears have set up a dedicated support line that is staffed to answer any questions this resident may have about the incident.

In response to this incident, the Bears have implemented additional security measures to help protect the privacy of information stored on its systems, including enhancing its multi-factor

FOLEY

FOLEY & LARDNER LLP

authentication process, expanding existing technical and security controls, and providing additional privacy and cybersecurity awareness training to its staff.

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,

Aaron K. Tantleff
Foley & Lardner LLP

Encl: Sample Notification Letter

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<First_Name>> <<Last_Name>>:

We value and respect the privacy of your information, which is why, as a precautionary measure, we are writing to inform you of a recent security incident that involves some of your personal information. This letter contains information about what happened, the measures taken in response, and steps you can take to help protect your information. You are receiving this letter because you are a current or former player or employee of the Chicago Bears.

WHAT HAPPENED?

On February 14, 2024, we were alerted to suspicious activity associated with one of our employee's email accounts and immediately stopped it from continuing while it was still in progress. Upon becoming aware of this situation, we immediately secured the account and launched an investigation. The investigation determined that an unauthorized third-party accessed the employee's email account on February 14, 2024 and may have viewed certain data stored in the account during that time. As part of this investigation, we initiated a detailed review of the emails and attachments in the affected email account to identify whether personal information belonging to individuals may have been accessible to the unauthorized party. Our review concluded on February 29, 2024, at which time we determined that some of your personal information was contained within the impacted account at the time of the incident.

WHAT INFORMATION WAS INVOLVED?

The information involved in this incident includes your full name and one or more of the following types of health information: medical condition, diagnosis, injury or symptom-related details, medical history, procedure type, treatment information, medication, test results, patient account number, and/or medical record number.

WHAT WE ARE DOING.

Although we have no evidence of actual misuse of any of your information, we are notifying you out of an abundance of caution. In response to this incident, we implemented additional security measures to help protect the privacy of your information, including enhancing our multi-factor authentication process, expanding existing technical and security controls, and providing additional privacy and cybersecurity awareness training to our staff.

WHAT YOU CAN DO.

Although the information involved in this incident does not affect your credit, we are required by law to provide you certain information about identity theft. Please review the enclosed "Other Important Information" document included with this letter for further information.

FOR MORE INFORMATION.

For further information and assistance, please call Justin Stahl, VP of Information Technology, at 847-739-5257 or Brent Johnson, IT Security Architect, at 847-739-5355 between 9 a.m. - 5 p.m. Central Time, Monday to Friday.

Sincerely,

Justin L. Stahl

Justin Stahl

VP of Information Technology

The Chicago Bears Football Club, Inc.

OTHER IMPORTANT INFORMATION

Monitor Account Statements and Credit Reports. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, you should promptly notify the financial institution or company with which your account is maintained.

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the nationwide credit reporting agencies. To order your annual 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 from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213
- **Innovis**, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 1-800-540-2505

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the nationwide credit reporting agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 1-800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, https://www.innovis.com/personal/fraudActiveDutyAlerts, 1-800-540-2505

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 1-800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, 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 5 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. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. 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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338). This notice has not been delayed by law enforcement.

- ***For Maryland Residents***: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: (410) 576-6491 or (888) 743-0023.
- ***For Oregon Residents***: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.