

RECEIVED

APR 06 2026

CONSUMER PROTECTION

McDonald Hopkins PLC  
39533 Woodward Avenue  
Suite 318  
Bloomfield Hills, MI 48304

P 1.248.646.5070  
F 1.248.646.5075

Dominic A. Paluzzi  
Direct Dial: 248.220.1356  
Email: [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com)

April 3, 2026

**VIA U.S. MAIL**

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

**Re: New Orleans Louisiana Saints, LLC – Incident Notification**

To Whom It May Concern:

McDonald Hopkins PLC represents New Orleans Louisiana Saints, LLC (“Saints”). I am writing to provide notification of an incident at the Saints that may affect the security of personal information of approximately one (1) New Hampshire resident. By providing this notice, the Saints do not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

As a result of a cybersecurity incident, the Saints learned that an unauthorized actor gained access to our network environment. Upon learning of this issue, the Saints immediately worked to contain the threat and secure its internal environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal information and was compromised as a result of this incident. After an extensive forensic investigation and complex manual document review, we discovered on March 4, 2026 that the impacted systems, which were accessed between July 16, 2025, and August 15, 2025 contained personal information. The information impacted included individual’s name and Social Security Number.

The Saints wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. The Saints providing the affected resident with written notification of this incident commencing on or about April 3, 2026, in substantially the same form as the letter attached hereto. The Saints are offering the resident with Social Security numbers impacted a complimentary one-year membership with a credit monitoring service. Additionally, the Saints have advised the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The resident was also provided with best practices to protect personal information, such as placing a fraud alert and/or security freeze on their credit files and obtaining a free credit report. The affected resident was also provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority to the Saints. The Saints are committed to maintaining the privacy of personal information in their possession and have taken many precautions to safeguard it. The Saints continually evaluate and modify their practices to enhance the security and privacy of the personal information they maintain.

If you have any additional questions, please contact me at (248) 220-1356 or [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com)

Sincerely,



Dominic A. Paluzzi

Encl.

New Orleans Louisiana Saints, LLC

[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]  
[REDACTED]

[REDACTED]

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to New Orleans Louisiana Saints, LLC ("Saints"). We are writing with important information regarding a data security incident. As such, we want to provide you with information about the incident, let you know the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

As a result of a cybersecurity incident, the Saints learned that an unauthorized actor gained access to our network environment.

What We Are Doing.

Upon learning of this issue, we immediately worked to contain the threat and secure our internal environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been compromised as a result of this incident. After an extensive forensic investigation and complex manual document review, we discovered on March 4, 2026 that the impacted systems, which were accessed between July 16, 2025, and August 15, 2025, contained some of your personal information as described in more detail below.

What Information Was Involved?

The information involved includes your [REDACTED]

What You Can Do.

We have no knowledge that your information has been or will be misused as a direct result of this incident. Out of an abundance of caution and to protect you from potential misuse of your information, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for [REDACTED] months.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our toll-free response line at [REDACTED]. The response line is available Monday through Friday, [REDACTED] m. Eastern Time.

Sincerely,

New Orleans Louisiana Saints, LLC  
5800 Airline Dr  
Metairie, LA 70003

[REDACTED]

- OTHER IMPORTANT INFORMATION -

**1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring.**

To help protect your identity, we are offering complimentary access to Experian IdentityWorks for [REDACTED] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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).

Please note that Identity Restoration is available to you for [REDACTED] months 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 [REDACTED]

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [REDACTED]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by [REDACTED] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [REDACTED]
- Provide your activation code: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by [REDACTED]. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

**2. Obtain and Monitor Your Credit Report**

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228**, visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), 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 access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### **3. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

#### ***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

#### ***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

#### ***TransUnion***

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

### **4. Placing a Security Freeze on Your Credit File.**

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

#### ***Equifax Security Freeze***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888)-298-0045

#### ***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

#### ***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

## 5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

\*\*\*\*

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: 515-281-5164.

**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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://www.ncdoj.gov/), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Washington D.C. Residents:** You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

**New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA). These 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.ftc.gov/system/files/ftc\\_gov/pdf/fcra-may2023-508.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf) or [www.ftc.gov](http://www.ftc.gov).

*In Addition, New Mexico Consumers Have the Right to  
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.