



Jackson Lewis P.C.
666 Third Avenue
29th Floor
New York, NY 10017
(212) 545-4063
www.jacksonlewis.com

Damon W. Silver
Direct: (212) 545-4063
damon.silver@jacksonlewis.com

By Email: idtheft@oag.state.md.us

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

Re: Data Incident Notification¹

September 22, 2023

Dear Sir or Madam:

We are writing to notify your office that Frax Outsourcing, a subsidiary of TheKey, LLC (“Frax”), was the subject of a criminal cyberattack (the “Incident”) that impacted files stored in a legacy system used by Frax. We immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through our extensive investigation, we identified a limited set of email accounts and a SharePoint drive in the Frax environment that may have been subject to unauthorized access. We then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those accounts and that drive to determine whether they contained personally identifiable information (“PII”) and to identify the data subjects to whom that PII related.

On or about June 19, 2023, we determined that the threat actor(s) may have accessed PII in the affected accounts related to a specific set of individuals during the period of November 2 to November 15, 2022. The impacted accounts contained names, along with social security numbers, medical information, government ID numbers and/or driver’s license numbers. We found no evidence that this information was misused.

The investigation identified 148 Maryland residents that may have been affected by the Incident. Out of an abundance of caution, and in accordance with applicable law, we will provide notice to the affected Maryland residents, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused.

¹ Please note that Frax Outsourcing, a subsidiary of TheKey, LLC, does not, by providing this letter, agree to the jurisdiction of the State of Maryland, nor waive its right to challenge jurisdiction in any subsequent actions.

As set forth in the enclosed letter, Frax has taken a number of steps to further secure its systems. Specifically, it has migrated from the legacy Frax environment all active data and email accounts and fully decommissioned that environment.

We will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.

Sincerely,

JACKSON LEWIS, P.C.

/s/ *Damon W. Silver*

Damon W. Silver

cc: Melissa Pascualini (Jackson Lewis P.C.)

EXHIBIT A



Frax Outsourcing
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/fraxoutsourcing>

September 21, 2023

Notice of Data Breach

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

What Happened

We are writing to notify you that Frax Outsourcing, a subsidiary of TheKey, LLC (“Frax”), was the subject of a criminal cyberattack (the “Incident”) that impacted files stored in a legacy system used by Frax. We immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through our extensive investigation, we identified a limited set of email accounts and a SharePoint drive in the Frax environment that may have been subject to unauthorized access. We then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those accounts and that drive to determine whether they contained personally identifiable information (“PII”) and to identify the data subjects to whom that PII related.

On or about June 19, 2023, we determined that, during the period of November 2 to November 15, 2022, the threat actor(s) may have accessed PII in the affected accounts that related to you. We have not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The impacted files may have contained your name, along with your <<Data Elements>>.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-577-6462, going to <https://response.idx.us/fraxoutsourcing> or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am – 6 pm Pacific Time. Please

note the deadline to enroll is December 21, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have taken a number of steps to further secure our systems. Specifically, we have migrated from the legacy Frax environment all active data and email accounts and fully decommissioned that environment.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We apologize for any inconvenience this Incident may cause you. Please call 1-888-577-6462 or go to <https://response.idx.us/fraxoutsourcing> for assistance or for any additional questions you may have.

Sincerely,



Terrence Vetter
Head of Information Security & Infrastructure
TheKey, LLC

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.

You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.

Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
800-525-6285
securitymonitoring@equifax.com

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
888-397-3742
businessrecordsvictimassistance@experian.com

TransUnion
Consumer Relations & Fraud
Victim Assistance
P.O. Box 2000
Chester, PA 19016
800-372-8391
databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580

4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.
5. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State’s Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
6. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.
7. *For Oregon Residents:* You can obtain information about steps you can take to help prevent identity theft from the Oregon Department of Justice at: [Identity Theft - Oregon Department of Justice: Consumer Protection \(state.or.us\)](http://Identity Theft - Oregon Department of Justice: Consumer Protection (state.or.us)).

