

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
kevin.scott@gtlaw.com

July 9, 2024

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

Dear Attorney General Brown:

We represent FPL Food LLC ("FPL") located at 1301 New Savannah Rd, Augusta, GA 30901, and are writing to notify your office of an incident that may affect the security of some personal information relating to 4 Maryland residents.

Recently, FPL was the target of a ransomware attack. FPL immediately notified law enforcement, moved quickly to contain the incident, and conducted a thorough investigation with the assistance of computer forensic experts. While FPL believes it is likely the attacker only wanted money and not the information on its computers, in an abundance of caution, they are notifying the entire data population that their information may have been accessed by the attackers.

On June 14, 2024, FPL discovered that data containing personal information was exfiltrated from its IT environment. While FPL has no reports of misuse of anyone's information, its investigation revealed that the system may have contained information relating to personal information, and it took time to identify those persons affected. The information may have included individuals' name, address, Social Security number, and employee benefits information.

The security of all information in FPL's systems is taken very seriously, and they want to assure that there are already steps in place to prevent a reoccurrence, including implementing increased security measures and conducting additional employee training. Additionally, FPL is offering individuals one year of identity protection (credit monitoring and identity theft) services from Kroll.

On or about July 3, 2024, FPL began mailing notifications to all potentially affected individuals. An example of the notification is attached. Notification has also been made to the three major credit reporting agencies.

Should you have any questions regarding this notification or other aspects of the data security event, please contact me for any additional information.

Attorney General Brown

July 9, 2024

Page 2

Best Regards

A handwritten signature in blue ink, appearing to read "Kevin M. Scott", with a long horizontal flourish extending to the right.

Kevin M. Scott
Shareholder



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

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

<<b2b_text_1 (Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

We are writing to inform you of a data security incident that may have impacted some of your personal information. We take the security of your information and any concern this incident may cause very seriously. This letter contains information about actions we have taken to prevent a reoccurrence, and steps you can take to help protect your information.

What Happened?

Recently, we were the target of a ransomware attack. Ransomware is a computer virus that encrypts computer systems until and unless we pay money (i.e., the ransom) demanded by the attackers. We immediately notified law enforcement, moved quickly to contain the incident, and conducted a thorough investigation with the assistance of computer forensic experts. We believe it is likely the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that some of your personal information may have been accessed by the attackers.

What Information was Involved?

Our investigation revealed that some documents accessed may have contained information including your name, address, Social Security number, and employee benefits information.

What Are We Doing?

The security of all information in our systems is taken very seriously, and we want to assure you that there are already steps in place to prevent a reoccurrence, including implementing increased security measures and conducting additional employee training.

Additionally, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

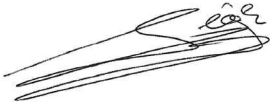
What You Can Do.

Although we have no reports of misuse of your or anyone's information, we encourage you to follow the instructions in this letter and activate the identity monitoring services we are providing at no cost to you. We also recommend that you review the "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For More Information.

If you have any questions, please call [1-800-828-8888](tel:1-800-828-8888), Monday through Friday from 9:00 am - 6:30 pm Eastern Time, excluding major U.S. holidays. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "F. Leger", written over a horizontal line.

Francois Leger
Chief Executive Officer



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit 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.

Additional Important Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Attorney General
400 6 th Street NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov

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

Massachusetts and Rhode Island residents: You have the right to obtain or file a police report.

For residents of all states: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348-5788 www.equifax.com/personal/credit-report-services/credit-freeze/ 1-866-478-0027	P.O. Box 9554 Allen, TX 75013-9544 http://www.experian.com/freeze/center.html 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze 1-800-916-8800