Maria Efaplomatidis, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C 402
Brooklyn, NY 11201
mefaplomatidis@constangy.com

March 27, 2024

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith, and Prophete LLP represents July Business Services ("JULY") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in compliance with Maine's data breach notification statute.

1. Nature of the Security Incident

On November 13, 2023, JULY identified unusual activity in its email environment. In response, JULY immediately conducted an investigation and took steps to contain the incident. In so doing, JULY engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. Through that investigation, JULY learned of information suggesting that an unknown actor gained unauthorized access to our email environment on November 14, 2023, and potentially accessed or acquired certain files, some of which may have contained personal information. On February 26, 2024, it was determined that certain personal information may been accessed or acquired without authorization.

2. Number of Affected Maine Residents Notified

On March 27, 2024, JULY notified 31 Maine residents by letter mailed via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

The impacted information may include the residents' names and social security numbers.

3. Measures Taken to Address the Incident

In response to the incident, JULY retained cybersecurity experts and launched a forensics investigation to determine the source and scope thereof. JULY implemented additional

security measures to further harden its environment in an effort to prevent a similar event from occurring in the future.

JULY is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose personal information was affected by this event, including 12 months of Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Those services are offered through Kroll. Kroll will also support a call center for at least 90 days to answer questions and assist with enrollment.

4. Contact Information

JULY takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 718.719.6475 or mefaplomatidis@constangy.com.

Sincerely yours,

Maria Efaplomatidis of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Encl.: Sample Consumer Notification Letter

<<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 (Subject: Notice of Data [Breach / Security Incident])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

July Business Services ("JULY") is writing to inform you of a data security incident that may have involved your personal information. JULY is a financial planning services company that provides support to employers such as <<b2b_text_2 (Client Name)>> and its employees. JULY takes the privacy and security of your personal information very seriously. Therefore, we are writing to inform you about the incident and advise you of certain steps that you can take to help protect your personal information.

What Happened? On November 13, 2023, we identified unusual activity in our email environment. In response, we immediately conducted an investigation and took steps to contain the incident. In so doing, JULY engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. Through that investigation, we learned of information suggesting that an unknown actor gained unauthorized access to our email environment on November 14, 2023 and potentially accessed or acquired certain files, some of which may have contained personal information. On February 26, 2024, it was determined that your personal information may been accessed or acquired without authorization.

What Information Was Involved? The potentially affected information may have included your name along with your social security number.

What We Are Doing? As soon as we discovered the incident, we engaged third-party experts to conduct a complete and thorough investigation. JULY also enhanced the security of its email environment to prevent a similar incident from occurring in the future.

Although we have no evidence that your information has or will be misused as a result of this incident, we are providing you with information about steps you can take to help protect your information. Additionally, we are offering you complimentary identity monitoring services for 12 months through Kroll, a national leader in identity monitoring services. 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.

With this monitoring service, Kroll will help you resolve issues if your identity is compromised.

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

You have until <<b2b_text_6 (activation date)>> *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. We encourage you to activate the complimentary identity monitoring services we are offering. With this service , Kroll can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information. Kroll Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding holidays. Please call the help line at <<Telephone Number>> and supply the specialist with your membership number listed above.

Protecting your information is important to us. Please know that we take this incident very seriously, and we deeply regret any worry or inconvenience this may cause you.

Sincerely,

July Business Services
Vice President, Business Development & Marketing
400 Austin Avenue, Suite 1200
Waco, Texas 76701

KROLL

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.

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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).

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification 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. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

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.

Federal Trade Commission	**Maryland Attorney General**	**New York Attorney General**
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 1-212-416-8433

North Carolina Attorney General	**Rhode Island Attorney General**	**Washington D.C. Attorney General**
9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 1-401-274-4400	441 4th Street, NW Washington, DC 20001 oag.dc.gov 1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.