

May 21, 2026

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: Notice of Data Security Incident—Update

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP represents Sterling Seacrest Pritchard, Inc. (“SSP”) in connection with a recent data security incident described below. This notice is being sent on behalf of SSP because personal information for Maine residents could have been involved in the incident. SSP is also providing this notification on behalf of certain data owners that are clients of SSP.

This notice is being provided as an update to our prior submission provided on March 27, 2026.

I. NATURE OF THE SECURITY INCIDENT

As previously advised, SSP learned of unusual activity involving its email environment in August 2025. In response, SSP took measures to ensure its environment was secure. SSP also began an investigation, which revealed that certain data may have been accessed or acquired without authorization between August 12, 2025, and August 13, 2025.

SSP thereafter undertook a comprehensive review of the potentially affected information and worked to gather information needed to provide notice. This process concluded on March 19, 2026, and SSP worked to effectuate notifications to individuals for whom a data owner client of SSP could not be confirmed.

On April 14, 2026, SSP provided notification to data owner clients potentially involved to identify what personal information was impacted and to whom it belonged. SSP then worked with the data owner clients to effectuate notification to remaining individuals.

The potentially affected information varies for each individual but may have included individuals’ names and Social Security Number.

II. NUMBER OF MAINE RESIDENTS AFFECTED

As previously submitted, on March 25, 2026, SSP notified twenty (20) Maine residents within the potentially affected population, via USPS First-Class Mail. On May 19, 2026, SSP notified one (1) additional Maine resident within the potentially affected population, via USPS First-Class Mail.

III. ACTIONS TAKEN IN RESPONSE TO THE INCIDENT

As soon as SSP discovered the potential email issue, it took immediate steps to secure the affected email account, launched an investigation with the assistance of independent experts, and worked to determine

whether any personal information was accessed or acquired without authorization in connection with the incident. SSP thereafter worked diligently to determine what personal information may have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification.

SSP has established a toll-free call center through Kroll to answer questions about the incident and address related concerns. In addition, SSP is offering individuals whose Social Security numbers or driver's license information was involved twelve (12) months of complimentary credit and identity protection services through Kroll.

SSP is providing impacted individuals with guidance on how to protect against identity theft and fraud. SSP is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

IV. CONTACT INFORMATION

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,



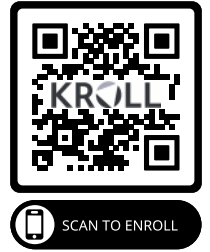
Aubrey L. Weaver
Partner, Cybersecurity & Data Privacy Team

Encl. Sample Consumer Notification Letter



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



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

<<b2b_text_1 (Re: Notice of Data Breach/Security Incident)>>

Dear <<first_name>> <<last_name>>:

Sterling Seacrest Pritchard (“SSP”) is writing to notify you of a data security incident which may have involved your personal information. SSP is an insurance brokerage and risk management firm that provides services to various employers. We held limited information related to you due to our relationship with <<b2b_text_3 (Company)>>. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened? On August 13, 2025, we discovered suspicious activity within our email environment. We promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. We engaged cybersecurity experts to conduct an investigation into what happened and to assist us with determining whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired between August 12, 2025 – August 13, 2025. We then completed a comprehensive analysis of the data potentially involved to identify what information was impacted and to whom it belonged. On or about April 14, 2026, we notified <<b2b_text_3 (Company)>> that information regarding some of their employees and related individuals was affected. We then coordinated with that entity to issue this notification to you.

Please note that we have no evidence of fraudulent misuse, or attempted misuse, of the potentially impacted information.

What Information Was Involved? The information that may have been involved in this incident includes your name as well as <<b2b_text_2 (Data Elements)>>.

What You Can Do. You can follow the recommendations included with this letter to protect your information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately. In addition, you can contact Kroll representatives who will work on your behalf to help resolve issues you may experience as a result of this incident.

What Are We Doing? As soon as the incident was discovered, we took the steps discussed above. To reduce the likelihood of a similar incident occurring in the future, we implemented additional measures to enhance the security of the network.

We are also providing you with access to <<ServiceTerminMonths>> months of credit monitoring and fully managed identity theft recovery services through Kroll. 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, 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 (Date)>> to activate your identity monitoring services.

Membership Number: <<Member ID (S_N)>>

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

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call (844) 403-4513 toll-free Monday through Friday from 8 am – 5:30 pm Central (excluding major U.S. holidays).

We take your trust in SSP and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

Sterling Seacrest Pritchard
2500 Cumberland Pkwy SE, Suite 400,
Atlanta, GA 30339

Steps You Can Take to Help 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 (the “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 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

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

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 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.

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

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
[www.marylandattorneygeneral.gov/
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
[www.doj.state.or.us/
consumer-protection](http://www.doj.state.or.us/consumer-protection)
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400
There were 5 RI Residents affected.

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf



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 will 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.

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.