Maria Efaplomatidis, Partner
Cybersecurity & Data Privacy Team
45 Main Street, Suite 206
Brooklyn, NY 11201
mefaplomatidis@constangy.com
Direct: 917.414.8991

January 13, 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
Tel: 207-626-8800

Re: Notice of Data Security Incident

Dear Attorney General Frey,

Constangy, Brooks, Smith & Prophete LLP represents Posillico, Inc. ("Posillico") in connection with a data security incident described in greater detail below. In reporting this matter, Posillico reserves all rights and defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, and personal jurisdiction.

1. **Nature of the incident.**

On December 8, 2025, Posillico discovered that it had experienced a network disruption and immediately initiated an investigation of the matter. Posillico engaged independent cybersecurity experts to assist with the process. As a result of the investigation, Posillico determined that certain files were potentially accessed or acquired without authorization. Posillico undertook a comprehensive review of those files to confirm the specific information involved so it could notify if required by law.

On January 6, 2026, Posillico learned that personal information belonging to certain Maine residents was contained within the affected files. Please note that Posillico is not aware of any fraud or misuse concerning the information involved in the incident.

2. **Number of Maine residents notified.**

Posillico notified 3 Maine residents of this incident via first-class U.S. mail on January 13, 2026. The information potentially impacted in connection with this incident includes name and Social Security number.

A sample copy of the notification letter is included with this correspondence.

3. **Steps taken relating to the Incident.**

As soon as Posillico discovered this incident, Posillico took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, Posillico implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. Posillico also reported this incident to the FBI's Internet Crime Complaint Center and will cooperate with any resulting investigation.

Posillico provided notified individuals with information about steps they can take to protect their personal information, and offered them access to complimentary identity monitoring services. Posillico also established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns.

4. Contact information.

Posillico remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please contact us.

Best regards,

Maria Efaplomatidis
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Posillico

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

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

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: April 12, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

January 12, 2026

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident experienced by Posillico, Inc. ("Posillico") that may have affected your personal information. Posillico and affiliated companies take the privacy and security of all information within their possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On December 8, 2025, Posillico discovered that it had experienced a network disruption and immediately initiated an investigation of the matter. Posillico engaged independent cybersecurity experts to assist with the process. As a result of the investigation, Posillico and affiliated companies determined that certain files were potentially accessed or acquired without authorization. Posillico undertook a comprehensive review of those files and, on or about January 6, 2026, learned that some of your personal information was contained in the files which is the reason for this notification. Please note that Posillico has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name and <<Variable Text 2: Impacted Data Elements>>.

What We Are Doing. As soon as Posillico discovered this incident, it took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. Posillico is also offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is April 12, 2026.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through IDX by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-837-3805 Monday through Friday from 9 am - 9 pm Eastern Time. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Posillico, Inc.

Steps You Can Take to Help Protect Your Personal Information

1. Website and Enrollment. Scan the QR image or go to http://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-837-3805 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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	**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 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
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
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

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.