

February 19, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP, represents Pond & Company ("Pond") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you, in accordance with Maine's statute, that this incident may have affected the personal information of 2 Maine residents.

1. Nature of the Security Incident

On May 26, 2023, Pond became aware of potential unauthorized access to its network. Upon discovering this activity, Pond's internal security teams took immediate steps to secure its network. Pond also engaged a team of leading external cybersecurity experts to assist in its response and conduct an investigation to determine what happened and what information may have been involved.

The investigation revealed that between March 29, 2023 and April 5, 2023, an unauthorized actor acquired certain Pond data. As a result, Pond undertook a comprehensive review of the potentially affected data. Pond's review concluded on December 24, 2023, at which time Pond determined that the data contained certain personal information. Since then, Pond has been working to gather contact information needed to provide individual notification.

2. Number of Maine Residents Involved

On February 14, 2024, Pond notified 2 Maine residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

The personal information involved in this incident includes name, Social Security number, driver's license number, and passport number.

3. Steps Taken to Address the Incident

As soon as Pond discovered this unauthorized activity, it took steps to secure the affected system and launched an investigation to determine whether, and to what extent, personal information had been accessed or acquired without authorization. Pond also reported the matter to the FBI and will provide whatever cooperation is necessary to hold the perpetrator accountable.

Pond has implemented additional measures to enhance its network security and minimize the risk of a similar incident occurring in the future. Further, as referenced in the sample consumer notification letter, Pond is providing individuals with complimentary credit and identity protection services.

4. Contact Information

Pond remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (806)-535-0274 or by e-mail at lnickle@constangy.com. Please let me know if you have any questions.

Sincerely,



Lindsay B. Nickle
Vice Chair
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample 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(Re: Notice of Data Security Incident / Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

I am writing to inform you of a data security incident that may have affected your personal information. Please note that Pond & Company (“Pond”) has no evidence that your information has been misused. At Pond, we take the privacy and security of personal information very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to activate your complimentary credit monitoring and identity monitoring services.

What Happened. On May 26, 2023, Pond became aware of potential unauthorized access to its network. Upon discovering this activity, our internal security teams took immediate steps to secure our network. We also engaged a team of leading external cybersecurity experts to assist in our response and conduct an investigation to determine what happened and what information may have been involved.

The investigation revealed that between March 29, 2023 and April 5, 2023, an unauthorized actor acquired certain files and data stored within our systems. As a result, we launched a comprehensive review of the potentially affected data and identified that some of your information may have been involved. Since then, we have been working to gather contact information necessary to provide you with this notice.

What Information Was Involved. The potentially affected information may have included your <<b2b_text_2(data elements)>>.

What We Are Doing. As soon as Pond discovered the incident, we took the steps described above. Pond also reported the matter to the FBI and will cooperate with any resulting investigation. Further, Pond implemented additional measures to enhance our network security and minimize the risk of a similar incident occurring in the future.

Additionally, to help relieve concerns and to help protect your identity following this incident, Pond is offering you 12 months of complimentary credit monitoring and identity monitoring services through Kroll, global leader in risk mitigation and response. Your services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.¹

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>>

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. You can also activate the Kroll identity monitoring services, which are offered to you at no cost, using the instructions above. Please note the deadline to activate these complimentary services is <<b2b_text_3(enrollment deadline)>>. Please do not discard this letter, as you will need the Activation Number provided above to access services.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

For More Information. Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call [\[Toll Free Number\]](#) Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Kroll representatives are fully versed on this incident and can answer any questions or concerns you may have.

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,

Pond Management
Pond & Company
3500 Parkway Lane, Suite 500
Peachtree Corners, GA 30092



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

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
1-800-916-8800
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.

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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

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