

EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Jones & Beach Engineers, Inc. (“Jones & Beach”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 23, 2024, Jones & Beach discovered suspicious activity related to an employee’s email account. Jones & Beach launched an investigation and engaged third-party forensic specialists to determine the nature and scope of the activity. Their investigation determined that there was unauthorized access to an email account on December 27, 2023, and then January 12, 2024, to January 23, 2024. Thereafter, Jones & Beach undertook a comprehensive and time-intensive review of the contents of the email account to determine what information was contained therein and to whom it related. On March 29, 2024, Jones & Beach finalized this review and determined that certain sensitive information was located within the emails and attachments subject to unauthorized access.

The information that could have been subject to unauthorized access for Maine residents includes name and Social Security number.

Notice to Maine Residents

On May 15, 2024, Jones & Beach provided written notice of this incident to two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Jones & Beach moved quickly to investigate and respond to the incident, assess the security of Jones & Beach systems, and identify potentially affected individuals. Jones & Beach is also working to implement additional safeguards and training to its employees. Jones & Beach is providing access to credit monitoring services for two (2) years, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Jones & Beach is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Jones & Beach is providing individuals with information on how to place a fraud alert and security freeze on one’s 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.

Jones & Beach is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

JONES & BEACH ENGINEERS INC.

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

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

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

Jones & Beach Engineers, Inc. (“Jones & Beach”) is writing to inform you of a recent incident that may impact the security of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the incident, our response, and steps you may take to protect against any misuse of your information, should you feel it necessary to do so.

What Happened? Earlier this year, Jones & Beach discovered suspicious activity related to an employee’s email account. We launched an investigation and engaged third-party forensic specialists to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to an email account on December 27, 2023, and then January 12, 2024, to January 23, 2024. Thereafter, the Jones & Beach team undertook a comprehensive and time-intensive review of the contents of the email account to determine what information was contained therein and to whom it related. On March 29, 2024, we finalized this review and determined that information related to you was located within one of the emails or attachments subject to unauthorized access.

What Information Was Involved? The information contained in the impacted accounts included your <<b2b_text_1 (name + Data Elements)>>.

What We Are Doing. Jones and Beach takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the issue, we immediately commenced an investigation to confirm the nature and scope, and to identify what information could have been affected.

As an added precaution, we are offering you access to twenty-four (24) months of complimentary identity monitoring services through Kroll at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the activation process yourself as we are not permitted to activate these services for you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. We further encourage you to activate the complementary services being provided through Kroll.

For More Information. We understand you may have questions about the incident that are not addressed in this letter.

If you have questions, please call 1-???-???-???, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,



Wayne G. Morrill
President

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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 (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.

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.

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.