

Jena M. Valdetero
Tel 312.456.1025
Fax 312.456.8435
valdeteroj@gtlaw.com

January 28, 2022

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Notification of Security Incident

Dear Attorney General Formella:

We represent Bard Associates, Inc. (“Bard Associates”). We are writing to inform you that Bard Associates has notified two (2) individuals who reside in New Hampshire of a data security incident that may have affected some of their personal information.

On January 10, 2022, Bard Associates became aware of a cybersecurity incident in which an unauthorized third party gained access to the email account of one of Bard Associates’ employees. Upon further investigation, we identified unauthorized access to a second employee’s mailbox, through which an unauthorized party had redirected certain emails starting on July 8, 2021. Upon discovery, Bard Associates immediately worked to contain the incident and identify potentially affected individuals. The affected email accounts may contain information about certain of Bard Associates’ current and former clients, which could include some or all of the following: names, addresses, birthdates, Social Security numbers and brokerage account numbers.

Bard Associates takes the security of its clients’ personal information very seriously and has taken steps to prevent a reoccurrence of this event. These steps include disabling the unauthorized individual’s access to the affected email accounts, further improving access controls for employees, enhancing deployment of its multifactor authentication efforts, changing all passwords to its email system, increasing the monitoring of its networks, hardening its systems, notifying its custodian financial organizations, and requesting enhanced monitoring from these organizations for any unusual requests regarding Bard Associates client accounts.

Bard Associates initially provided notice to its clients via email on January 12, 2022 and followed up via a second email with a credit monitoring offer on January 21, 2022, in order to immediately enable individuals to take steps to protect themselves, should they determine it is necessary. Bard Associates also mailed notification letters to all potentially affected individuals beginning January 21, 2022. A copy of the notification letter is attached.

Office of the Attorney General

January 28, 2022

Page 2

Bard Associates is offering identity theft protection services through a data breach and recovery service, IDX. Services include 24 months of triple bureau credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Please contact me for any additional information.

Best Regards,

A handwritten signature in blue ink that reads "Jena Valdetero". The signature is written in a cursive, flowing style.

Jena Valdetero
Shareholder

JMV:

Notice of Data Breach

Dear Client,

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code:
A2XZBKE5GU

Timothy B. Johnson

*135 South LaSalle Street
Suite 3700
Chicago, Illinois 60603
Tel: 312 782-9600
Fax: 312 782-3785
Tim@bardassociatesinc.com*

As you may know, Bard Associates, Inc. (“Bard”) recently experienced a data security incident that may have exposed some of the personal information of our investors and employees. We take the security of your personal information very seriously and sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to help prevent a reoccurrence, and steps you can take to protect your information.

What Happened

On January 10, 2022, Bard became aware of a cybersecurity incident in which an unauthorized third party gained access to my email account to send a fraudulent invoice request to my assistant. Upon further investigation, we discovered that, in addition to the brief unauthorized access on January 10th to my mailbox, someone had gained access to my assistant’s account and had copied certain emails starting on July 8, 2021. We immediately responded to and worked to contain the incident, alerted law enforcement, and began investigating with the assistance of third-party cybersecurity experts. Although it is our policy to never send sensitive information in emails without password protection, and we have no indication at this time that your information was misused, we are notifying you because we cannot rule out the possibility that misuse could occur.

What Information Was Involved

Personal information that could be contained within the affected mailboxes may include: your name, brokerage account numbers, social security numbers, addresses, and date of birth. As we previously advised, emails sent to my administrative assistant between July 8, 2021, and January 10, 2022, containing certain terms regarding a wire or payment were automatically forwarded to an unauthorized third party. If you have any questions about whether a particular email you sent during this time may have been forwarded, please contact Michael Demaray.

What We Are Doing

We take the security of personal information very seriously, and we want to assure you that we’ve already taken steps to help prevent a reoccurrence. We have disabled the unauthorized individual’s access to the affected email accounts, further improved access controls, changed all passwords to our email system, notified our custodian financial organizations asking them to monitor for any unusual requests regarding client accounts, increased the monitoring of our networks, and strengthened our systems and procedures.

In addition, we are offering complimentary identity theft protection services through IDX. This includes two years of triple credit bureau monitoring and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Sign up instructions are included with this letter, but if you need help please let us know.

Additional information describing IDX’s services is included with this letter.

(Over)

What You Can Do

We recommend that you review the enclosed Recommended Steps document. This document describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you should always remain vigilant and closely monitor your personal accounts for any suspicious or unusual activity. You may also want to implement dual factor authentication for your personal accounts where possible. As an added precaution, we can have your account number changed with your custodian if you would like. Please contact Michael if you want to do this. Both Fidelity and Schwab have a good system that uses your voice to identify you if you call them, so set this up if you have not done so already.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. They will be ready for your call on Tuesday, January 25th. Please note the deadline to enroll is April 24, 2022.

You can also obtain information about identity theft and how to protect yourself through resources available through the Federal Trade Commission:

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338), www.identitytheft.gov

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call Michael Demaray, at 312-782-9600 for assistance in enrolling in these services.

We regret any concern or inconvenience this incident may cause and are committed to continuing to take steps to help protect the information entrusted to us.

Sincerely,



Timothy B. Johnson
President
Bard Associates, Inc.

(Enclosure)



Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to <https://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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Additional Important Information

For residents of Iowa: Please report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: Please report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: Please review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights pursuant to the federal Fair Credit Reporting Act. Please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General

441 4th Street NW
Washington, D.C.
20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General

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

Rhode Island Office of Attorney General

150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Attorney General

9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.com

New York Attorney General

120 Broadway
3rd Floor
New York, NY
10271
1-800-771-7755
www.ag.ny.gov

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

(Over)

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. You only need to contact one credit bureau; they will then notify the other two of the fraud alert request.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. Unlike a fraud alert, you need to make a credit freeze request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
<https://www.experian.com/help/>
1-888-397-3742

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/>
1-800-525-6285

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016-0200
<https://www.transunion.com/credit-help>
1-800-680-7289