



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Robert H. Bender, Jr.
Senior Counsel
D: 215.650.6619
Robert.bender@fmglaw.com

September 23, 2024

VIA Email

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Subject: Notice of Data Event

Dear Sir or Madam,

We represent East Shore Sound, Inc. located at PO Box 512, Jarrettsville, MD 21084, and we write to notify your Office of a recent event that may impact the security of information relating to 27 Maryland residents. By providing this notification, East Shore Sound does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

In April 2024, East Shore Sound identified unusual activity within its network. East Shore Sound promptly investigated the activity and determined it was the victim of a ransomware attack. On May 17, 2024, the investigation determined the cybercriminals responsible for the attack accessed documents from the network before deploying malware. East Shore Sound reviewed these documents and determined some of them included human resources files containing employee information. East Shore Sound thereafter conducted a comprehensive review of these locations to determine what information was present and the corresponding individuals. After completing the review, East Shore Sound reviewed available records to confirm contact information for these individuals so it could notify them as appropriate. On September 9, 2024, East Shore Sound completed the review and determined the impacted population included 27 Maryland residents.

On September 23, 2024, East Shore Sound provided written notice of this incident to 27 Maryland residents. Notice is being provided in substantially the same form as the letter attached as ***Exhibit A***. The impacted information varied by individual but included name, address, Social Security number, driver's license or state identification number, and passport number.

East Shore Sound is providing notified individuals access to complimentary identity monitoring services. East Shore Sound is also provided individuals with guidance on how to protect against identity theft and fraud, including information on how to place a fraud alert and/or security freeze, the contact details for the national consumer reporting bureaus, information on how to obtain a free credit report, a reminder to remain vigilant against possible identity theft and identify by reviewing account statements and 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.

Upon identifying unusual system activity, East Shore Sound took prompt steps to secure its network and to investigate the activity. These efforts included engaging forensic specialists to investigate the attack and prioritizing restoring its network and operations in a safe, effective, and secure manner. East Shore Sound continues to assess its network security, including updating policies and procedures as appropriate. East Shore Sound also reported the event to the FBI and intends to cooperate with any subsequent investigation.

If you have questions about this notification or the data security event, please contact us at 215-650-6619.

Very Truly Yours,

FREEMAN MATHIS & GARY, LLP

A handwritten signature in blue ink that reads "Robert H. Bender, Jr." The signature is written in a cursive, flowing style.

Robert H. Bender, Jr.

Enclosures

Exhibit A



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

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

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

September 23, 2024

Re: Notice of Data Event

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

East Shore Sound, Inc. values your privacy and security. As part of that commitment, we are notifying you of a recent data security event affecting your information. This letter provides a summary of the event, our response, and steps you can take to protect your information, including enrolling in complimentary identity monitoring we are offering.

What Happened?

In April 2024, we discovered activity within our network we determined was from a malware attack. We partnered with computer forensic specialists to investigate the nature and scope of the event. On May 17, 2024, our investigation confirmed the cybercriminals responsible for the attack accessed documents from the network. We reviewed these documents and determined some of them included human resources files containing certain employee information. Therefore, we are notifying applicable employees and providing them with enclosed resources.

What Information Was Involved?

You are receiving this letter because your <<Variable Data 1>> was present within HR files on our network at the time of the event. We have no indication that any of your information was misused, but we are notifying you and providing resources so you may take steps to protect your information, should you find it appropriate to do so.

What We Are Doing.

Upon discovery of the network disruption, we investigated immediately to assess the risk to data on our network and restored our network in a safe and efficient manner to minimize disruptions. We notified federal law enforcement and intend to cooperate with any investigation. We also continue to review the existing policies and security measures in place for ways to enhance the protection of data on our network. As an added precaution, we are offering you 12 months of complimentary identity monitoring services through IDX, A ZeroFox Company. Enrollment instructions are enclosed in the following pages. The deadline to enroll is December 23, 2024.

What You Can Do.

We encourage you to remain vigilant against identity theft and fraud, including reviewing and monitoring your account statements and credit reports. You should report errors or suspicious activity to your financial institution or the appropriate service provider. You can also enroll in the complimentary identity monitoring services. Please refer to the enclosed documentation titled "Steps You Can Take to Help Protect Information" for available resources.

For More Information

We understand you may have questions. Please contact our dedicated assistance line at 800-939-4170 between 9:00 AM and 9:00 PM, Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'W. Saltzer', enclosed within a thin black rectangular border.

William ("Bill") Saltzer
President
East Shore Sound, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

1. Website and Enrollment. Scan the QR image or 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.

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax
1-888-378-4329
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
1-888-397-3742
P.O. Box 4500
Allen, TX 75013
www.experian.com

TransUnion
1-800-916-8800
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online using the above contact information. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online using the above contact information. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

You can obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-ID-THEFT (438-4338). This notification was not delayed by law enforcement.
- **Maryland residents:** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; <https://www.marylandattorneygeneral.gov/> or 1-410-528-8662 or 1-888-743-0023. East Shore Sound is located at PO Box 512, Jarrettsville, MD 21084.

- ***New Mexico residents:*** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what information is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by contacting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.
- ***New York residents:*** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov>; or 1-800-771-7755.
- ***North Carolina residents:*** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; <https://ncdoj.gov>; and toll-free at (877) 566-7226 or (919) 716-6000.
- ***Rhode Island residents:*** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag.ri.gov or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately [0] Rhode Island residents potentially impacted by this incident.