

MARY T. COSTIGAN
DIRECT DIAL: (908) 795-5135
EMAIL: MARY.COSTIGAN@JACKSONLEWIS.COM

June 27, 2024

VIA ELECTRONIC MAIL

Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident¹

Dear Sir or Madam:

Please be advised that our client, Atlantic States Marine Fisheries Commission (“ASMFC” or the “Commission”), learned that personal information of approximately one thousand ninety-four (1,094) Maryland residents may have been subject to unauthorized access or acquisition as the result of a ransomware attack (the “Incident”). ASMFC is located at 1050 N. Highland Street, Suite 200A-N, Arlington, VA 22201.

With assistance from third-party experts, ASMFC took immediate steps to secure its systems, restore operations, and conduct a forensic investigation into the nature and scope of the Incident. Based on the investigation, it appears the Incident began on or about March 14, 2024 and ended on April 6, 2024, the date ASMFC discovered the attack. The Commission promptly notified law enforcement. After reviewing the investigation results, ASMFC concluded that unauthorized actor(s) may have gained access to certain ASMFC files containing personal or confidential information. For purposes of the Maryland state data breach notification law, the data elements of personal information involved may have included: name, mailing address, email address, phone number, Social Security number, bank account and routing number, SSN copies of ID cards (driver's license, Social Security cards, birth certificate and/or passport). ASMFC has worked diligently to identify contact information for potentially impacted individuals and has commenced its notification process via U.S. mail.

Additionally, as an added precaution, ASMFC is also offering potentially affected individuals a chance to enroll in complimentary identity theft protection services through IDX, A

¹ Please note that by providing this letter ASMFC is not agreeing to the jurisdiction of State of Maryland, nor waiving its right to challenge jurisdiction in any subsequent actions.

ZeroFox Company. IDX identity protection services include Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Instructions for enrollment in this complimentary service are included in the notification letter, a draft of which is also enclosed for reference.

Since the Incident, ASMFC has taken steps to augment its safeguards and will continue to review its privacy and data security policies and procedures to minimize the chances of any similar reoccurrences.

Should ASMFC become aware of any significant developments concerning this situation, we will inform you. If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS, P.C.

/s/ Mary T. Costigan

Mary T. Costigan

200 Connell Drive, Suite 2000

Berkeley Heights, NJ 07922

PH: (908) 795-5135

FX: (908) 464-2614

mary.costigan@jacksonlewis.com

MTC

Enclosure



Atlantic States Marine Fisheries Commission

1050 N. Highland Street • Suite 200A-N • Arlington, VA 22201
703.842.0740 • www.asmfc.org

Joseph Cimino (NJ), Chair

Dan McKiernan (MA), Vice-Chair

Robert E. Beal, Executive Director

Sustainable and Cooperative Management of Atlantic Coastal Fisheries

June 26, 2024

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

RE: Notice of Data Breach

Dear [Name]:

We are writing to notify you that Atlantic States Marine Fisheries Commission (“ASMFC”) experienced a cybersecurity incident (“Incident”) that may have involved your personal information. In this letter, we describe what happened, how we are handling the Incident, and who you can contact with questions.

What Happened

On April 6, 2024, ASMFC learned it was the victim of a cybersecurity incident that affected our organization’s electronic systems. ASMFC promptly notified law enforcement. With assistance from third-party experts, we took immediate steps to secure our systems, restore operations, and investigate the nature and scope of the Incident. Based on our investigation, the Incident appears to have begun on or about March 14, 2024 and ended on April 6, 2024.

What Information Was Involved

As part of our extensive forensic investigation, we have worked diligently to determine whether any personally identifiable information may have been impacted. We have concluded that some or all the following information may have been subject to unauthorized access and acquisition during the Incident: name, mailing address, email address, phone number, Social Security number, bank account and routing number, copies of ID cards (driver's license, Social Security cards, birth certificate and/or passport).

What We Are Doing

We apologize for any concern this Incident may cause you. ASMFC recognizes the importance of safeguarding your personal information. As part of our ongoing focus on cybersecurity, we have augmented our security practices to minimize the risk of a similar incident occurring in the future. At the end of this letter we have included several precautionary steps you may wish to take to safeguard your personal information.

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

As an added precaution, we are also offering you a chance to enroll in complimentary identity theft protection services through IDX, A ZeroFox Company. IDX identity protection services include 24 months of Credit and

MAINE • NEW HAMPSHIRE • MASSACHUSETTS • RHODE ISLAND • CONNECTICUT • NEW YORK • NEW JERSEY • DELAWARE
PENNSYLVANIA • MARYLAND • VIRGINIA • NORTH CAROLINA • SOUTH CAROLINA • GEORGIA • FLORIDA

CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

What You Can Do

You can enroll in the free IDX identity protection services by going to <https://app.idx.us/account-creation/protect>, calling 1-866-329-9984, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is October 18, 2024.

Please note that at this time, we have no evidence that your information has been misused. However, we encourage you to take full advantage of this offered service.

For More Information

You will find additional instructions for enrolling at the end of this letter. When enrolling, you will need to reference the enrollment code, so do not discard this letter.

If you have any questions, please call us at 703.842.0740.

Sincerely,



Robert Beal

Enrollment Information and Additional Steps and Resources To Help Protect Your Personal Information

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

- 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.
- Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. 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 and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact all the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you send a written request by regular, certified or overnight mail to the three credit reporting agencies. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone. In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the

identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

4. Contact your local law enforcement, your state attorney general, or the Federal Trade Commission if you suspect or know that you are the victim of identity theft.

You also have the right to file a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you may need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items.

You can also contact the Fraud Department of the FTC. The Fraud Department will collect your information and make it available to law enforcement agencies.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580
(877) 438-4338

5. Obtain additional information about identity theft.

- *All US residents:* Obtain consumer assistance and educational materials on identity theft, privacy issues, and avoiding identity theft from the Federal Trade Commission (“FTC”) at www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338.
- *Connecticut Residents:* Contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- *Maryland Residents:* Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.
- *New York Residents:* Contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State’s Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
- *North Carolina Residents:* Obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877566-7226, www.ncdoj.gov.
- *Rhode Island Residents:* Contact the Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. If you are a victim of identity theft, you may file a police report by contacting your local police department. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.

- *Washington D.C.:* You may also contact the Attorney General for the District of Columbia at <http://oag.dc.gov/>; 441 4th St. NW, Washington, D.C. 20001; Telephone: (202)-727-3400.