

9 March 2023

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



Via regular mail and e-mail: Idtheft@oag.state.md.us

Dear Sir/Madam

This letter is sent to you pursuant to Md. Code Com. Law § 14-3501. On January 23, 2023 A10 Networks, Inc. ("A10") criminal actors targeted A10's shared internal drives, deployed "Play" malware and impacted data focused on legal, finance, and HR functions. A10 discovered the event on January 23rd, contained it within a few hours, and engaged in a subsequent investigation and forensic analysis by CrowdStrike.

In the days since the event A10 has undertaken the following actions:

- *Engaged CrowdStrike and deployed its Falcon endpoint detection service and forensic collection tools to the A10 environment;*
- *Completed necessary activities to enable normal computing services;*
- *Completed network updates and related corrective actions.*

Although A10's presence in Maryland is very small (we only have four employees in the state) on February 10, 2023 we notified them of the event and offered to provide at no cost, credit monitoring services to all such individuals. A copy of that notification is attached along with an attachment that went with it titled "Recommended Steps to Help Protect Your Information."

Please feel free to contact us if you need additional information and/or have any questions.

Yours faithfully,

For and on behalf of A10 Networks, Inc.

Scott Weber
General Counsel
2300 Orchard Parkway
San Jose, CA 95131
USA



Scott Weber

From: Andrew Kim
Sent: Friday, February 10, 2023 9:06 AM
To: All_US-DL
Subject: Cyber Security Incident
Attachments: Recommended Steps to Help Protect Your Information[1].pdf

Importance: High

Team,

As you are aware, A10 experienced a cybersecurity incident on January 23, 2023, and our preliminary analysis has determined that criminal actors accessed shared internal drives, deployed malware and impacted data focused on legal, finance, and HR functions.

What information was involved?

While our investigation has not been completed yet, we believe there is a risk that employee personal data theft has occurred. Our cybersecurity partner is working quickly to identify the specific categories and types of data that were taken. We have not yet determined whether sensitive details were taken.

What are we doing?

- Because there is a risk this has occurred, as a precautionary measure, we have arranged with third-party credit monitoring services to offer identity protection services to all A10 personnel and their families.
- We have also implemented changes in processes and tools to strengthen for heightened threat monitoring.
- Once our investigation is complete, we will be sending affected employees formal data breach notifications, to report further on what personal details were taken as to individual employees.

We are offering, at no cost to you, identity theft protection services for you and your family including dependents or beneficiaries up to 5 members through IDX, a data breach and recovery services expert. IDX identity protection services include 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and managed ID theft recovery services. IDX can help you resolve issues if your or your family's identity is compromised.

To enroll, please visit: <https://app.idx.us/account-creation/protect> and use the enrollment codes below:

12-month 1B Monitoring/CyberScan/Insurance/Restoration - FAMILY

Enrollment code: IB3JKFMVG

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

Enrollment window: 2/9/23 – 6/9/23

12-month 1B Monitoring/CyberScan/Insurance/Restoration - INDIVIDUALS

Enrollment code: IB3S56I4Z

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

Enrollment window: 2/9/23 – 6/9/23

What Else You Can Do

We encourage you to contact IDX with any questions and to enroll your family in the free identity protection services described herein 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 6 am - 6 pm Pacific Time. Please note the deadline to enroll is June 9, 2023.

We encourage you to, and hope you will, take full advantage of this service.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment codes above when enrolling, so please do not discard this email.

If you have any questions, please send your questions directly to [HelloHR@A10networks.com](mailto>HelloHR@A10networks.com)

Sincerely,

Andrew Kim

Vice President, Worldwide Human Resources



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. Note, only one adult can use the enrollment code above. Once you have enrolled, you can add a second adult and up to five minors by going to the account detail tab and adding them under Family Management. The second adult will receive an invite to setup their own member portal and the minors will be listed under the account that used the enrollment code.

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. 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.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. 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.

5. 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 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.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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 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 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 agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.