



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 23, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Systems Application & Technologies, LLC d/b/a SA-TECH ("SA-TECH") located at 1101 Mercantile Lane, Unit 200, Upper Marlboro, Maryland 20774, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three hundred twenty-two (322) Maryland residents. This notice may be supplemented should any new significant facts be learned subsequent to its submission. By providing this notice, SA-TECH 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.

Nature of the Data Event

On March 26, 2024, SA-TECH first became aware of suspicious activity affecting certain systems within its network. SA-TECH immediately launched an investigation into the nature and scope of the incident with the assistance of industry leading cybersecurity specialists. The investigation determined that certain files and folders within SA-TECH's network were accessed and/or taken without authorization between March 20, 2024 and March 26, 2024. Therefore, out of an abundance of caution, SA-TECH conducted a comprehensive and time-intensive review, with the assistance of third-party data review specialists, of the contents of the files to determine whether sensitive information was involved and to whom it related. SA-TECH then engaged in an extensive internal reconciliation and validation effort for the information obtained. This review was recently completed.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license or state identification number, financial account information, and health information.

Notice to Maryland Residents

On or about October 23, 2024, SA-TECH provided written notice of this incident to three hundred twenty-two (322) Maryland 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, SA-TECH moved quickly to investigate and respond to the incident, assess the security of SA-TECH systems, and identify potentially affected individuals. Further, SA-TECH notified federal law enforcement regarding the event. SA-TECH is also working to implement additional safeguards and training to its employees. SA-TECH is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SA-TECH is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SA-TECH 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.

SA-TECH is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,

A handwritten signature in black ink, appearing to read 'EJ Finn', is enclosed in a thin black rectangular border.

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/kzm
Enclosure

EXHIBIT A



0002073

Systems Application and Technologies, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB-09551

9_0002073



**Systems Application
& Technologies, Inc.**

[REDACTED]
[REDACTED]
[REDACTED]



October 23, 2024

Notice of Security Incident

Dear [REDACTED]:

Systems Application & Technologies, Inc. ("SA-TECH") is writing to notify you of an incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this event, this letter provides details of the incident, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On March 26, 2024, SA-TECH first became aware of suspicious activity affecting certain systems within our network. We immediately launched an investigation into the nature and scope of the incident with the assistance of industry leading cybersecurity specialists. The investigation determined that certain files and folders within our network were accessed and/or taken without authorization between March 20, 2024 and March 26, 2024. Therefore, out of an abundance of caution, SA-TECH conducted a comprehensive and time-intensive review, with the assistance of third-party data review specialists, of the contents of the files to determine whether sensitive information was involved and to whom it related. SA-Tech then engaged in an extensive internal reconciliation and validation effort for the information obtained. This review was recently completed.

What Information Was Involved? Our review determined the following types of information related to you were involved in this incident: [REDACTED]. At this time, we have no indication that your information was used to commit identity theft or fraud as a result of this incident.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon becoming aware of this incident, we promptly commenced an investigation to determine the nature and scope of this incident. This investigation and response included, but was not limited to, assessing the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals for whom we had contact information. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, procedures and processes to reduce the likelihood of a similar future event. We will also notify, or have notified, applicable regulatory authorities where necessary.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statement and monitoring your credit free reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the information contained in the attached Steps You Can Take to Help Protect Personal Information. There you will also find more information on the complimentary credit monitoring services we are making available to you.

For More Information. If you have additional questions, please call our toll free hotline at 855-577-8539 Monday through Friday from 8:00 am to 8:00 pm EST (excluding U.S. holidays). You may also write to SA-TECH at 1000 Town Center Dr # 110, Oxnard, CA 93036.

Sincerely,

Systems Application & Technologies, Inc.

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 1 Rhode Island residents that may be impacted by this event.