



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Michele Veltri
Office: (267) 930-2297
Fax: (267) 930-4771
Email: mveltri@mullen.law

411 Theodore Fremd, Ste 206S
Rye, NY 10580

February 5, 2025

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 Aleto, Inc. ("Aleto") located at 1440 N Edgewood St, Suite 178, Arlington, Virginia 22201, and are writing to notify your office of an incident that may affect the security of certain personal information relating to forty (40) Maryland residents. By providing this notice, Aleto 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 or about December 24, 2024, Aleto became aware of suspicious activity related to one employee's device. Aleto immediately took steps to secure its network and launched an investigation to determine the nature and scope of the incident. The investigation determined that between December 20, 2024, and December 24, 2024, an unauthorized actor accessed an employee's device. Following this determination, Aleto reviewed the impacted device to determine the full extent of the information contained on the device subject to unauthorized access, in order to provide notice to impacted individuals and equip the individuals with information that may be helpful.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license, passport number, state identification card, other government identification number, medical information, and health insurance information.

Notice to Maryland Residents

On or about February 5, 2025, Aleto provided written notice of this incident to forty (40) 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, Aleto moved quickly to investigate and respond to the incident, assess the security of Aleto systems, and identify potentially affected individuals. Aleto is also working to implement additional safeguards and training to its employees. Aleto 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, Aleto is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Aleto is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Aleto is providing written notice of the event to relevant regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2297.

Very truly yours,

Michele Veltri of
MULLEN COUGHLIN LLC

MTV/mls
Enclosure

EXHIBIT A



Aleto, Inc
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS289



February 5, 2025

NOTICE OF SECURITY INCIDENT

Dear _____ :

Aleto, Inc. ("Aleto") is writing to notify you of an incident that may affect the privacy of some of your information. We are providing you with details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On December 24, 2024, Aleto became aware of suspicious activity related to one employee's device. Aleto immediately took steps to secure its network and launched an investigation to determine the nature and scope of the incident. The investigation determined that between December 20, 2024, and December 24, 2024, an unauthorized actor accessed an employee's device. Following this determination, we reviewed the impacted device and recently determined that your information was contained on the device and was potentially accessed or acquired by the unauthorized actor.

What Information Was Involved? The investigation determined the following types of your personal information may have been impacted by the incident: your name _____ Please note that we have no evidence that your personal information was subject to any actual or attempted misuse as a result of this incident.

What We Are Doing. We take this incident and the security of your information seriously. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies, procedures, and processes related to the storage of, and access to, personal information and are conducting additional workforce training to reduce the likelihood of a similar future incident.

As an added precaution, we are also offering _____ of complimentary access to credit monitoring services through Cyberscout, a TransUnion company. Individuals who wish to receive these services must enroll by following the instructions in the enclosed *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible misuse of your information, should you feel it appropriate to do so.

For More Information. We understand that you may have additional questions about this incident. Should any additional questions arise, please call 1-800-405-6108 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, and provide your unique code in the enclosed *Steps You Can Take to Help Protect Your Information*.

Sincerely,

Aleto, Inc.



Steps You Can Take To Help Protect Your Information

Enroll in Monitoring Services

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 _____ 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: _____. 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Internal Revenue Service Identity Protection PIN (IP PIN)

You may also obtain an Identity Protection PIN (“IP PIN”) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects misuse of your personal information. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application, or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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/>. You may also write to Aleto at 1440 N Edgewood St, Suite178, Arlington, VA 22201.

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.