



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienna@mullen.law

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

March 30, 2023

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 AudienceView Ticketing Corporation (“AudienceView”) located at 200 Wellington Street West, 2nd Floor, Toronto, Ontario M5V 3C7, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three hundred twenty nine (329) Maryland residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AudienceView 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 February 21, 2023, AudienceView discovered suspicious activity within a certain digital product it provides which is embedded into the website of its clients. AudienceView immediately initiated an investigation into the nature and scope of the event and determined that its product was impacted with malware. The investigation determined that between February 14, 2023, and February 21, 2023, certain individuals’ information may have been subject to unauthorized access and acquisition as they submitted payment card information. In response, AudienceView moved quickly to remove the malware from its product and reviewed the affected data in order to identify what information is contained therein and to whom that information relates. On February 21, 2023, AudienceView completed its review and determined that personal information related to certain individuals may have been impacted by this event. AudienceView worked diligently since this time to confirm the contact information for the individuals. In the interim, AudienceView provided notice to the individuals via electronic mail on February 28, 2023. Additionally, AudienceView is currently performing a full investigation into the incident with the assistance third party forensic specialists.

Mullen.law

The information potentially impacted by this event includes name, billing address, e-mail address, and payment card information.

Notice to Maryland Residents

On March 28, 2023, AudienceView provided written notice of this incident to three hundred twenty nine (329) 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, AudienceView moved quickly to investigate and respond to the incident, assess the security of its product, and identify potentially affected individuals. Further, AudienceView notified federal law enforcement regarding the event. AudienceView also implemented additional safeguards and is providing access to credit monitoring services for one (1) year through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, AudienceView 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. AudienceView 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.

AudienceView 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) 930-4259.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CDS/myc
Enclosure

EXHIBIT A



2540 Walden Avenue
Suite 450
Cheektowaga NY 14225

00766-SONTIQ G0244 L003 AUTO 005001

[REDACTED]

March 27, 2023

NOTICE OF SECURITY INCIDENT

Dear [REDACTED],

AudienceView Ticketing Corporation ("**AudienceView**") is writing to notify you of an incident that may have impacted the privacy of some of your personal information. AudienceView is a cloud-based ticketing solution that enables organizations to sell tickets and other functionalities. AudienceView serves as a vendor to [REDACTED]. We sincerely apologize that this incident occurred, and are providing you with information about the incident, our response to it, and resources we are making available to you to help protect your information, should you wish to do so.

What Happened? On February 21, 2023, AudienceView discovered suspicious activity within our Campus product which is embedded into the website of [REDACTED]. We immediately initiated an investigation into the nature and scope of the event and determined that our Campus product was impacted with malware. The investigation determined that between February 14, 2023, and February 21, 2023, certain individuals' information may have been subject to unauthorized access and acquisition. In response, we moved quickly to remove the malware from our Campus product and reviewed the potentially impacted data in order to identify what information is contained therein and to whom that information relates. Based on our investigation to date, we understand that personal information related to you may have been impacted by this incident.

What Information Was Involved? The investigation determined that your name, billing and shipping address, e-mail address, and payment card information may have been impacted by this event.

What Are We Doing? The confidentiality, privacy, and security of personal information is among AudienceView's highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to remove the malware, secure our systems, and launched a full investigation with the assistance of third-party forensic specialists. We have implemented additional security measures to further protect against similar incidents occurring in the future. We also reported this incident to federal law enforcement and are cooperating with their investigation.

Additionally, we are offering credit monitoring and identity protection services for 12 months through CyberScout, Inc., a TransUnion company ("TransUnion"), at no cost to you. The deadline to enroll in these services is June 28, 2023. Please note that you will not be automatically enrolled in these services. Should you wish to do so, you will need to enroll yourself in these services, as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the enclosed Steps You Can Take to Help Protect Personal Information.

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

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please call our dedicated assistance line at 1-833-806-1882 between the hours of 9:00 a.m. and 6:30 p.m., Eastern Time, Monday through Friday, excluding major U.S. holidays. You may also write to AudienceView at 200 Wellington Street West, 2nd Floor, Toronto, Ontario M5V 3C7.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,
Gord Dyer
Chief Financial Officer
AudienceView Ticketing Corporation

DEV

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Restoration

We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a 12-month subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

[\[REDACTED\]](#)

You will be prompted to enter the following activation code:

Please ensure that you redeem your activation code before 6/28/2023 to take advantage of the service.

Upon completion of the enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to \$1,000,000 in coverage to protect against potential damages related to identity theft and fraud¹.
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-694-3367.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in

your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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 you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, 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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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, DC 20001; 202-727-3400; and oag@dc.gov. AudienceView is located at 200 Wellington Street West, 2nd Floor, Toronto, Ontario M5V 3C7.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. AudienceView is located at 200 Wellington Street West, 2nd Floor, Toronto, Ontario M5V 3C7.

For 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 bureaus 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 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. We encourage you to 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.

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/>. AudienceView is located at 200 Wellington Street West, 2nd Floor, Toronto, Ontario M5V 3C7.

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. AudienceView is located at 200 Wellington Street West, 2nd Floor, Toronto, Ontario M5V 3C7.

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, you have the right to obtain any police report filed in regard to this incident. There are 36 Rhode Island residents impacted by this incident.

DEV